G Data InternetSecurity 2014

ユーザーマニュアル

目次

はじめに **4**
ユーザーサポートについて 4

インストール **6**
インストール後 6

セキュリティセンター **14**
ステータス 14
ライセンス 14
ソフトウェアの機能 14

アンチウイルス **25**
ウイルススキャン 25
隔離されたファイル 25
ブートメディア 25

ファイアウォール **30**
ステータス 30
ネットワーク 30
ルールセット 30

フィルタリング **45**
新規ユーザー 45
禁止するコンテンツ 45
許可するコンテンツ 45
インターネット利用時間の監視 45
コンピュータ利用時間の監視 45
パーソナルフィルタ 45
設定|ログ 45

オートスタートマネージャー **58**
プロパティ 58

設定 **61**
一般 61
アンチウイルス 61
ファイアウォール 61

ログ **111**
アンチウイルスのログ 111
ファイアウォールのログ 111
フィルタリングのログ 111

FAQ: ブートスキャン **112**
ブートスキャンの準備 112
ブートスキャンの流れ 112

FAQ: 各種機能について 117
G Data アイコン 117
ウイルススキャンの流れ 117
ウイルス検出時の対応 117
ファイアウォールアラート 117
ウイルススキャンで「not-a-virus」が表示される 117
アンインストールの方法 117
FAQ: ライセンスについて 127
複数台用ライセンスを所有している場合 127
ライセンスの期限が切れた場合 127
コンピュータを買い替えたり、クリーンインストールした場合 127
データ保護に関する声明 127
使用許諾契約・コピーライト 127

はじめに

この度はG Data 製品をお買い求めいただき、誠にありがとうございます。本マニュアルでは、製品のインストール、コンピュータを不正プログラムから効果的に保護するためのヒントが分かりやすく纏められています。本製品を操作する上でわからないことがでてきたら、まずは、マニュアルやG Data ウェブサイトのFAQなどでご確認ください。

このマニュアルでは、製品のインストール方法と実用的なヒントをまとめています。

本マニュアルで使用されている画像はトータルプロテクションのものです。

メモ: 各機能の使用方法を簡単に調べたい場合はオンラインヘルプが便利です。オンラインヘルプは各画面にあるヘルプボタンを押すことで表示できます。

ユーザーサポートについて

操作方法など、ご購入後の製品に関するお問い合わせは、ユーザーサポートで受付いたします。

※体験版の場合は、ユーザーサポートのご利用はできません。予めご了承ください。

ユーザーサポートの連絡先

問い合わせ先については、登録後のメールをご確認ください。

1. サポート期間

ライセンス有効期間内

2. サポート範囲

製品のご利用の説明、疑問点にお答えするサービスとさせていただきます。以下の場合には、お問い合わせに対してのご回答ができませんので、予めご了承ください。

a) 本製品で保証している動作環境外でのお問い合わせ
b) 本製品ではないもの（ハードウェア・他社製品）に関するお問い合わせ
c) サポート時間外のサポートおよび、指定された方法以外の方法でのサポートのご依頼

3. ユーザーサポートをお受けになる際に

お問い合わせの際は、お客様番号または、レジストレーション番号をご用意いただき、更に質問要点を整理していただいた上で、お問い合わせいただきますようお願いいたします。

インストール

まず本製品をインストールする環境についてご確認ください。本製品を正常に機能させるためには、以下の**動作環境**を満たす必要があります。

動作環境

対応OS	Windows 8 (32bit/64bit) Windows 7 (32bit/64bit) Windows Vista (32bit/64bit) Windows XP [SP2以降](32bit) ※インストールには管理者(Administrator)権限でログインする必要があります。 ※日本語OS環境のみサポート。 ※最新のサービスパックを推奨。
CPU	各OSが推奨するCPU
メモリ	Windows 8/7/Vista：1GB以上 [2GB以上推奨] Windows XP：512MB以上 [1GB以上推奨] ※グラフィックメモリとの共用は除きます。
ハードディスク	1GB以上の空き容量
デバイス装置	CDドライブ（パッケージ版のみインストール時に必要） ※ブートCDの作成・バックアップ時には書き込み可能なCD/DVDドライブが必要です。
ディスプレイ	解像度1024×768ドット、High Color（16ビット、65,536色）以上
その他	InternetExplorer8以上 インターネットに接続可能な環境[ブロードバンド以上を推奨]

※他のウイルス対策ソフトとは併用できません。
※ユーザー登録するためにはPCのメールアドレス（携帯メール不可）が必要です。
新品のコンピュータ、もしくは本製品インストール前に他のウイルス対策ソフトで保護されていたコンピュータでは、次のステップを参考に本製品をインストールしてください。それ以外の場合やコンピュータがウイルスに感染している疑いがある場合は、インストール前にブートスキャンを実行することをお勧めします。 ブートスキャンの方法については、**ブートスキャンの流れ**を参照してください。

> **注意**: 本製品をインストールしようとしているコンピュータに、他社製のウイルス対策ソフトがインストールされている場合は、**必ず他社製品をアンインストールした後で、本製品をインストールしてください。**ウイルス対策ソフトは Windows のシステム深くに配置されて動作しするため、複数の製品を同時に使用すると深刻な問題が出る場合があります。
> なお、他社製品をアンインストールする場合、通常アンインストールではデータのゴミが残る場合がほとんどで、動作不良の原因となります。製品ごとに用意されている、**完全アンインストールツール**を使用してアンインストールする事で、コンピュータをクリーンな状態にでき、その上で本製品をインストールする事で最適な動作をさせることができます。他社製品の完全アンインストールツールに関しては、各社のユーザーサポートをご利用ください。

ステップ1 - インストールの開始

本製品はCD/DVD版もしくは、ダウンロード版として販売されています。それぞれのインストール方法は次の通りです:

- **CD/DVD 版の場合**: 本製品CD/DVDをドライブにセットします。
- **ダウンロード版の場合**: ダウンロードしたファイルをダブルクリックします。

しばらくすると、自動的にインストール開始画面が開きます。

> **注意**: インストールの起動画面が自動的に表示されない場合は、

Windowsの自動再生機能が無効になっているため、CD/DVD から本製品のインストール画面が自動的に起動しない可能性があります。

- 自動再生の画面が表示される場合は、**AUTOSTRT.EXE の実行** をクリックしてください。
- 自動再生の画面が開かない場合は、Windows 上で本製品のディスクを探して開き、**Setup** もしくは **Setup.exe** をダブルクリックしてください。

ステップ2 - インストール方法の選択

ウィザードにしたがってインストール処理を始めます。まず、標準インストール、もしくはユーザー自身でインストール内容を決定できるカスタムインストールを選択する画面が表示されますので、希望するインストール方法を選択してください。なお、通常は標準インストールを使用する事をお勧めします。

カスタムインストールを選択した場合は、自分の希望に応じてプログラムの保存場所やインストールする機能を選択する事ができます。

マルウェア情報イニシアチブ: G Data セキュリティラボでは、G Data 製品の利用者をコンピュータの安全性を脅かす脅威から保護するため、保護・対策の研究や分析に絶え間なく励んでいます。 マルウェア研究では、マルウェアに関する情報が多ければ多いほど、効果的な保護メカニズムの開発をいち早く進めることができます。これらの情報をG Data の研究・分析・開発に効率的に取り入れることを可能にするための取り組みが、G Dataマルウェア情

報イニシアチブです。 これにより、マルウェアに関するデータをG Dataセキュリティラボに送信することができます。 より多くのユーザー様に参加頂くことで、他のG Data製品をご利用の方々もインターネットをより安全に利用できるようになります。このインストール方法の選択画面にあるチェックボックスで、このデータを提供するかどうかの選択ができます。

ステップ3 - 使用許諾契約

使用許諾契約書をご確認いただき、同意できる場合は「同意してインストール」をクリックしてください。

ステップ4 - カスタムインストール (オプション)

カスタムインストールを選択した場合は、次の2つの画面でプログラムをインストール場所と、インストールする機能の範囲を指定することができます。標準インストールを選択した場合は、この手順は省略されます。

あらかじめ設定されているインストール範囲には以下の違いがあります:

- **ユーザー定義**: この設定ではソフトウェアの機能（例: アンチウイルス、アンチスパムなど）の横にあるボックスをチェックして、インストールする機能を自分で指定することができます。G Data アンチウイルス、G Data インターネットセキュリティ、またはG Data トータルプロテクション、それぞれの製品に応じて、ここで選択できる機能の種類は変わります。

- **完全**: 製品に含まれる全ての機能がインストールされます。
- **最小**: ウイルス対策に最低限必要な、アンチウイルス機能のみがインストールされます。

本製品のインストール後に、あとからインストールされている機能を変更する事も可能です。セットアップを起動し、**変更**を選択すると、カスタムインストールの要領で機能の追加や削除を行う事ができます。

ステップ5 - 製品種類の選択

この手順では、本製品を製品版として使用するか、体験版として試用するかを選択します。

- **製品版として登録**: 製品版を購入した場合は、ここを選択します。
- **体験版として登録**: 無料体験版として利用する場合は、ここを選択します。なお、体験版を利用するには、氏名とメールアドレスの入力が必要です。入力されたメールアドレスには、アクセスデータが送付されるので、必ず有効なPC用メールアドレスを入力してください。

ステップ6 - ライセンスの認証

インストール中に**ライセンスの認証**を行い、プログラムの機能をすべて使用できるようにします。

- **レジストレーション番号を入力**: 製品を新規購入された方は、ここを選択し、購入した製品のレジストレーション番号を入力してください。パッケージ版を購入された場合は、レジストレーション番号は同梱の用紙に記載されています。ダウンロード版を購入された場合は、レジストレーション番号はメールなどで送信されています（購入したWEBストアによって異なります）。

  注意: レジストレーション番号を入力して、製品が正常に認証されると、更新ファイルをロードできるようになります。複数台版やライセンスの移行で必要になるアクセスデータは、認証後に G Data から送付されるメールに記載されています。アクセスデータは厳重に保管してください。

  入力したレジストレーション番号で認証できない場合は、まず入力ミスの可能性がないか確認してください。それでも問題が解決できない場合は、**ユーザーサポート**にお問い合わせください。

- **アクセスデータを入力**: アクセスデータ（ユーザー名とパスワード）を使って、認証します。本製品を再インストールしたり、他のコンピュータでライセンスを認証したい場合（複数ユーザー版の場合など）は、ここを選択してアクセスデータを入力してください。

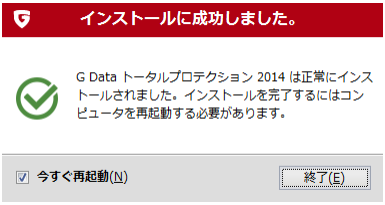
  注意: アクセスデータは初回認証（レジストレーション番号を入力）後に G Data から送付されたメールに記載されています。製品には同梱されていません。

  アクセスデータを紛失したり忘れた場合は、**アクセスデータの確認**をクリックしてください。ブラウザが自動的に起動して G Data のサポートページが開きます。サポートページに記載されている手順に沿って手続きをし、アクセスデータを再確認してください。※アクセスデータの再確認では、レジストレーション番号が必要です。またレジストレーション番号の登録時に使用したメールアドレスを変更した場合は、**ユーザーサポート**へお問い合わせください。

- **後で認証を行う**: 後で製品を認証する場合はここを選択します。認証を行わない場合はワクチン更新が行われないため、最新の脅威に対して適切な保護を提供する事ができなくなります。インストール後はできるだけ早く認証の手続きをしてください。インストール後の認証は、ワクチン更新を実行しようとした際に表示されるウインドウか、設定アイコンをクリックして、**アンチウイルス**の**更新**領域などから行う事ができます。

ステップ7 - インストールの完了

最後に、インストールを完了するためにコンピュータを再起動する必要があります。再起動が完了すると本製品が使用可能になります。



インストール後

インストール後には、ショートカットやタスクバーのアイコンから本製品を起動できるようになり、各種セキュリティ機能が利用可能になります：

G Data ショートカット: 左のアイコンがデスクトップ上に作成されます。本製品のインターフェースを開くには、このアイコンをダブルクリックします。セキュリティセンターの利用方法については、**セキュリティセンター**に詳しく記載しています。

G Data アイコン: ユーザーの操作が必要になると、タスクバーのG Data アイコンからお知らせします。このアイコンを右クリックして起動を選択する事で G Data のインターフェイスを開く事ができます。その他の情報は、G Data アイコンの項を参照してください。

G Data シュレッダー: インストールでシュレッダーを選択すると、デスクトップ上にシュレッダーアイコンが作成されます。シュレッダーを使ってファイルを完全に削除するには、ファイルをシュレッダーのアイコン上に移動するか、ファイルの上で右クリックして、シュレッダーを選択します。一旦シュレッダーでファイルを削除すると、ファイルは復元不可能になります。※シュレッダー機能は、**G Data アンチウイルス**には含まれていません。

クイックスキャン: 特定のファイルやフォルダだけをウイルススキャンしたい場合は、プログラム画面を起動する必要はありません。対象の上で右クリックし、**ウイルススキャン**を選択すると、スキャンが実行されます。

本製品をインストールしてコンピュータを再起動した際に、Windows が起動しない場合: まずCD/DVDドライブに本製品CDが挿入されたままではないか確認してください。本製品CDは、ブートスキャン機能を搭載しているので、コンピュータの設定によっては、Windows 起動前にブートCD が起動している可能性があります。製品CDがCD/DVDドライブに挿入されていた場合は、CDを取り出し、コンピュータを再起動してください。Windows が通常通りに起動します。

ブートスキャンに関する詳細は、**ブートスキャンの流れ**の項を参照してください。

セキュリティセンター

本製品を起動すると立ち上がるセキュリティセンター画面では、各機能のステータスを確認したり、操作を実行できます。ウイルスなどの脅威に対する保護は、通常バックグラウンドで動作しますが、利用者の判断が必要になる場合はタスクバー上にその情報が表示されます。

セキュリティステータス

セキュリティステータスのアイコンを使用すると、ボタン操作ひとつでコンピュータの保護状況を簡単に改善できます。

このアイコンをクリックすると、コンピュータを守るための対策が提案されます。全てのセキュリティステータスが再び緑色に戻るまで対策を行い、保護レベルを改善してください。セキュリティステータスが全て緑色になれば、コンピュータの保護は最新の状態であり、セキュリティセンターでの作業も終了です。

緑色のチェックマーク＝すべて良好（システムは保護されています）

赤色のマーク＝今すぐに改善が必要（システムが危険にさらされている可能性があります）

灰色のマーク＝このセキュリティ機能は無効（例 アンチスパム機能を停止している）

黄色のマーク＝近いうちに改善が必要（例 ソフトウェアアップデートが利用可能）

本製品の全ての機能は、必要に応じて設定変更する事ができます。機能や設定の詳細についてはこのオンラインヘルプの各項目をご覧ください

共通機能

以下のボタンを使用すると、各機能共通の操作を行う事ができます:

設定: 設定画面を開くには、このボタンをクリックしてください。表示されている画面に応じた設定画面が表示されます。

ログ: このボタンをクリックすると、本製品が実行した動作のログ（ウイルスキャン、ウイルス検出、更新履歴など）を一覧表示できます。

本製品のウインドウ右上にあるこのボタンからは、以下の機能を利用できます:

ヘルプを表示: プログラムに関するオンラインヘルプを表示することができます。オンラインヘルプは各機能利用時に表示されるヘルプボタンからも表示可能です。

プログラムの更新: プログラム更新が利用できる場合は、このボタンをクリックする事で、ワクチン同様にプログラムファイルを更新できます。詳細は、更新の項を参照してください。

情報: 本製品のプログラムバージョンや登録されたレジストレーション番号を確認できます。ユーザーサポートを利用する際などにご活用ください。

ステータス

以下の項目から現在のセキュリティステータスの確認ができ、それぞれの項目をクリックし操作を実行することで、コンピュータの保護状況を改善できます:

リアルタイム保護

ウイルスガードはウイルスを常時監視するリアルタイムスキャン機能で、書き込みおよび読み取り処理を監視します。あるプログラムが不正な機能を実行したり、不正ファイルを拡散しようとすると、ウイルスガードがこれを防ぎます。ウイルスガードは最も重要なウイルス対策の 1 つですので、特別な理由が無い限り、常に有効にしておいてください。

- **ウイルスガードを無効にする**: 必要に応じてウイルスガードを無効化できます。例えば、大量のデータをハードディスク上のある場所から別の場所にコピーしたり、多くのメモリを必要とする演算プロセス（DVD のコピーなど）を実行する時には、ウイルスガードを無効にするとコンピュータのパフォーマンスが向上します。
  ただし、パフォーマンスのためにウイルスガードを無効化したい場合は、ウイルスガードを無効化する際や、アンチウイルスの設定画面から設定できる、セキュリティ / パフォーマンス のオプションを調整する事で、納得行くパフォーマンスを出せるか先に確認することをお勧めします。

  注意: ウイルスガードは必要な時だけ無効化してください。また、ウイルスガードが無効に設定されている間は、できるだけインターネットには接続しないようにし、CD、DVD、メモリカードまたは USB メモリなどに保存されている、スキャンをしたことのないデータにはアクセスしないように注意してください。

- **ふるまい検知を無効にする**: ふるまい検知（ビヘイビアブロッキング）は、ワクチンによる検出とは独立した、未知のウイルスを検出するための機能です。この機能は特別な理由が無い限り、常に有効にしておいてください。

- **詳細設定**: この機能に関する設定画面、設定 | アンチウイルス | リアルタイム保護 を開きます。

前回のアイドリングスキャン

前回コンピュータをアイドリングスキャンによってスキャンした日時が表示されます。この項目が赤色で表示されている場合は、できるだけ早くウイルススキャンを実行してください。※アイドリングスキャンが無効になっている場合は**前回のウイルススキャン**と表示されます。

- **コンピュータをスキャン**: コンピュータを数時間使わなくてもいい場合や、ウイルス感染の疑いがあり、すぐに結果を確認したい、といった場合には、ここからすぐにコンピュータ全体をスキャンできます。この全体スキャンの間もコンピュータは使用できますが、ここで実行されるスキャンはコンピュータの最大パフォーマンスを利用するため、他のアプリケーションのパフォーマンスにも影響を与えます。この機能の詳細はウイルススキャンの流れ の項を参照してください。

- **今すぐ実行**: アイドリングスキャンは、ウイルススキャンがユーザーの作業の邪魔にならないように、コンピュータが使われていない状態にのみ自動的に起動するスキャン機能です。アイドリングスキャン中にユーザーがコンピュータを利用すると、実行中のスキャンはすぐに休止状態となります。次のアイドリングスキャン実行日よりも先にスキャンを行いたい場合は、**今すぐ実行**を選択してください。
  仕事の休憩中などにアイドリングスキャンを自動実行したくない場合は、**アイドリングスキャンを無効にする**を選択して機能を無効化してください（非推奨）。

ファイアウォール

ファイアウォールは、外部の不正侵入からコンピュータを防御するため防御する機能で、インターネットやネットワークとコンピュータとの間で送受信されるデータを監視します。許可されていないデータの書き込みやダウンロードを検知すると、ファイアウォールが警告を発し、それらのデータ通信を阻止します。
※この機能はG Data インターネットセキュリティ、G Data トータルプロテクションで利用できます。

- **ファイアウォールを無効にする**: 必要に応じて、ファイアウォールを無効にします（非推奨）。コンピュータがインターネットやネットワークと接続されている環境では、不正な攻撃や侵入から保護されなくなりますのでご注意ください。

- **オートパイロットを無効にする**: **オートパイロット**は、ファイアウォールが許可／拒否するアプリケーションを自動的に判断し制御する機能です。通常は、この機能を有効にしてファイアウォールを利用することを

お勧めします。オートパイロットを無効にした状態でファイアウォールを使用する場合は、プログラムにルールを学習させ、ネットワーク環境に合わせて設定していく必要がありますので、上級者ユーザー以外は、オートパイロットを無効にしないでください。

- **詳細設定**: この機能に関する設定画面、設定 | ファイアウォール | 自動 を開きます。

ウェブ保護

インターネット利用中の保護を提供する**ウェブ保護**の有効／無効を切り替えます。ウェブ経由での感染が増加している現在、ウェブ保護は感染防止のための重要な機能です。ウェブ機能を有効にすると、ウェブサイト経由の感染やフィッシング詐欺などの脅威をアクセス前に未然に防ぎます。

インターネット閲覧中にウェブサイトが本製品によって脅威として検出されると、サイトの閲覧はブロックされ、ブラウザ画面に警告が表示されます。

- **ウェブ保護を無効にする**: ウェブ保護を無効にすると、ウェブサイトのチェックが無効になるため、ウェブサイトから大量にデータをダウンロードする際などにダウンロード時間を省略できます。また、ウェブ保護が無効中の状態も、ウイルスガードがコンピュータを感染から守ります。しかし、例外的ケースを除いては、ウェブ保護は有効に設定することをお勧めします。

- **例外を設定**: ウェブ保護は、不正コードが仕掛けられたウェブサイト、またはフィッシングなどの詐欺サイトからコンピュータを保護する機能です。しかし場合によっては、ウェブ保護を有効にすると、安全なサイトであるにも関わらず、ウェブページが正しく表示されないことがあります。そのような場合は、対象ページのアドレスをホワイトリストに例外登録してください。これにより、ウェブ保護がブロックしていたページが閲覧できるようになります。詳細については、例外の項を参照してください。

- **詳細設定**: この機能に関する設定画面、設定 | アンチウイルス | ウェブ保護 を開きます。

メール保護

メール保護機能は、送受信されるメールの内容や添付ファイルをスキャンし、ウイルス感染を防ぎます。ウイルスが検出された場合は添付ファイルを削除、

もしくはウイルスの駆除を行います。

- **メール保護を無効にする**: メールのスキャンを行いたくない場合は、ここを選択してください。ただし、その場合はメール経由のセキュリティリスクが大きく増えますので、特別な場合を除いてメール保護は有効に設定しておくことをお勧めします。

- **詳細設定**: この機能に関する設定画面、設定 | アンチウイルス | メールスキャン を開きます。

Microsoft Outlook: Microsoft Outlook には、専用プラグインがインストールされます。このプラグインは、メールスキャンで設定できる POP3/IMAP ベースの保護を提供し、これにより、Outlook 上でのウイルスチェックがより簡単に行えます。メールまたはフォルダのスキャンを実行するには、Outlook メニューバーの **[G Data] > [フォルダをスキャン]** を選択します。
※通常のメールスキャンと併用すると送受信に問題が出る場合がありますので、その際はPOP/IMAP/SMTPのスキャンを無効にしてください。

アンチスパム

スパム保護は、迷惑な広告メールや大量のスパムメールに対する対策機能です。G Data のスパム保護は、緻密に設定された判断基準をもとにスパム判定を行い、迷惑メールや迷惑メール送信者を効果的にブロックします。
※この機能はG Data インターネットセキュリティ、G Data トータルプロテクションで利用できます。

- **ログ: スパム**: スパムと判断されたメールに関する情報が一覧で表示されます。 **「更新」**をクリックすると、ステータス情報を更新できます。対象を選択して**「削除」**をクリックすると、指定したメールのログを削除できます。なお、ここで削除しても、メールプログラムで受信した実際のメールは削除されません。
  「ホワイトリストに登録」では、選択したメールの送信者をホワイトリストに入れ、それ以降はこの送信者からのメールに対するスパムチェックは省略されるようになります。逆に**「ブラックリストに登録」**へ移動すると、この送信者に対するメールは、以降、より入念なスパムチェックが行われるようになります。

- **ログ: スパム以外**: スパムではないと判断されたメールに関する情報が一覧で表示されます。 **「更新」**をクリックすると、ステータスを更新できます。対象を選択して **「削除」**を押すと、指定したメールのログを削除できます。なお、ここで削除しても、メールプログラムで受信した実際

のメールは削除されません。
「ホワイトリストに登録」では、選択したメールの送信者をホワイトリストに入れ、それ以降はこの送信者からのメールに対するスパムチェックは省略されるようになります。逆に**「ブラックリストに登録」**へ移動されると、この送信者に対するメールは、以降、より入念なスパムチェックが行われるようになります。

- **ホワイトリストを編集**: 特定の送信者からのメールアドレスやドメインをスパム扱いしないように設定できます。「ホワイトリスト」に登録するには、**「新規作成」**ボタンをクリックし、スパム扱いしたくない**メールアドレス**（例：newsletter@gdata.co.jp）または**ドメイン**（例：gdata.co.jp）を**送信者アドレス/ドメイン**の欄に入力します。すると、入力された送信者またはドメインからのメールは、スパムではないと判定されるようになります。
  また、**「インポート」**をクリックすると、既存のメールアドレスまたはドメインのリストをホワイトリストに追加できます。インポートするリストには、アドレスおよびドメインが 1 件 1 行ずつ、上から順に入力されている必要があります。データフォーマットは、Windows の「メモ帳」で作成できるようなテキスト形式（txt ファイル）を使用します。**「エクスポート」**からは、上述のホワイトリストをテキスト形式で書き出すことができます。

- **ブラックリストを編集**: 特定の送信者からのメールアドレスやドメインをスパム扱いするように設定できます。「ホワイトリスト」に登録するには、**「新規作成」**ボタンをクリックし、スパム扱いしたい**メールアドレス**（例：newsletter@gdata.co.jp）または**ドメイン**（例：gdata.co.jp）を**送信者アドレス/ドメイン**の欄に入力します。すると、入力された送信者またはドメインからのメールは、スパムと判定されるようになります。
  また、**「インポート」**をクリックすると、既存のメールアドレスまたはドメインのリストをブラックリストに追加できます。インポートするリストには、アドレスおよびドメインが 1 件 1 行ずつ、上から順に入力されている必要があります。データフォーマットは、Windows の「メモ帳」で作成できるようなテキスト形式（txt ファイル）を使用します。**「エクスポート」**からは、上述のブラックリストをテキスト形式で書き出すことができます。

- **アンチスパムを無効にする**: アンチスパムを無効します。コンピュータでメールを利用しない場合などに、この機能を利用してください。

- **詳細設定**: この機能に関する設定画面、設定 | アンチスパム | スパム

フィルタ を開きます。

前回のワクチン更新

ここでは、最後にインターネットからワクチンをダウンロードした日時が表示されます。ステータス情報が赤色で表示される場合には、できるだけ近いうちに、ワクチン更新を実行してください。ワクチンを更新するには、この項目をクリックし、プルダウン表示される**ワクチンの更新**を選択します。

- **ワクチンの更新**: デフォルト設定では、ワクチンの自動更新が行われように設定されています。今すぐに更新を手動実行する場合は、ここをクリックします。
- **自動更新を無効にする**: ワクチンの自動更新を無効にする場合はここをクリックします。特種なケースを除いて、自動更新は常に有効にしておいてください。
- **詳細設定**: この機能に関する設定画面、設定 | アンチウイルス | 更新 を開きます。

次回のワクチン更新

ここには、次回のワクチン更新までの時間が表示されます。ワクチンを更新するには、この項目をクリックし、プルダウン表示される**ワクチンの更新**を選択します。

- **ワクチンの更新**: デフォルト設定では、ワクチンの自動更新が行われように設定されています。今すぐに更新を手動実行する場合は、ここをクリックします。
- **自動更新を無効にする**: ワクチンの自動更新を無効にする場合はここをクリックします。特種なケースを除いて、自動更新は常に有効にしておいてください。
- **詳細設定**: この機能に関する設定画面、設定 | アンチウイルス | 更新 を開きます。

ライセンス

ワクチン更新が利用できるライセンスの有効期限を確認できます。

ウイルス対策ソフトにおいて、更新は非常に重要です。インターネット更新は必ず定期的に実行し、製品を常に最新の状態に保つように心がけてください。本製品はお手元のライセンスの有効期間が切れる前に、自動的にライセンス延長についてお知らせします。ライセンスの延長は、以下の手順で簡単に手続きできます。

ライセンスの有効期間が切れた場合

ライセンス期限が切れる数日前から、タスクバーにその旨を知らせるバルーンが表示されます。 このバルーンをクリックすると、ダイアログが開くので、ダイアログの説明に従い、簡単に更新をインターネット経由でできます。

保護する台数を増やす

使用中の製品の登録可能ユーザー数をさらに増やしたい場合は、更新時に別製品へと切り替えることができます。この項目をクリックすると手続き用のウェブページが開きますので、そこで詳細をご確認ください。

ソフトウェアの機能

本製品では以下の機能が利用できます（製品により使用できる機能が異なります）:

セキュリティセンター: セキュリティーセンターでは、利用者がマルウェアなどの脅威に素早く簡単に対応できるよう、コンピュータの保護に必要な情報を一目で確認できます。

アンチウイルス: アンチウイルス機能は、お使いのコンピュータをウイルスガードにより常時リアルタイムスキャンを行ったり、指定した方法に従ってコンピュータ全体のスキャンを行い、感染を防ぎます。スキャンにより隔離したファイルの確認や、Windowsを起動せずにマルウェアをスキャンできるブートメディアの作成も、この機能から行えます。

ファイアウォール: ファイアウォールは、外部の不正侵入からコンピュータを防御するため防御する機能で、インターネットやネットワーク

とコンピュータとの間で送受信されるデータを監視します。許可されていないデータの書き込みやダウンロードを検知すると、ファイアウォールが警告を発し、それらのデータ通信を阻止します。
※この機能はG Data インターネットセキュリティ、G Data トータルプロテクションで利用できます。

バックアップ: バックアップは、シンプルかつ簡単な操作で、大切な書類やデータをバックアップする機能です。日常生活は、オンライン音楽サービス、デジタルカメラや電子メールの活用など、ますますデジタル化しており、個人的なデータのバックアップの重要度も増しています。
ハードウェアの故障、過失によるデータ消失、あるいはウイルスやハッカーによるデータ損害に備え、コンピュータに保存されている音楽データ、写真/動画データ、メールデータなどのデータを定期的にバックアップしましょう。
※この機能は G Data トータルプロテクションで利用できます。

チューナー: チューナーを使用すると、簡単な操作で OS を最適化できます。チューナーは Windows Update の自動確認をはじめ、定期的なデフラグ、レジストリと一時ファイルの定期的なクリーンアップに至るまで、Windows システム内を整理し、処理速度を向上させるツールです。
※この機能は G Data トータルプロテクションで利用できます。

フィルタリング: フィルタリング機能は、お子様がコンピュータを使用する際などに、ウェブサイトを一定の基準で評価判別して排除したり、コンピュータの利用時間に制限をかける機能です。
※この機能はG Data インターネットセキュリティ、G Data トータルプロテクションで利用できます。

データセーフ: データセーフは個人情報等の機密データを保護するための金庫のような機能です。ハードディスクの追加パーティションのような感覚で簡単に利用できます。
※この機能は G Data トータルプロテクションで利用できます。

オートスタートマネージャー: オートスタートマネージャーは、Windows の起動時に自動起動するプログラムを管理する機能です。通常、それらのプログラムは OS 起動時に読み込まれます。オートスタ

ートマネージャーを使用すると、各プログラムごとに自動起動のタイミングを遅らせたり、起動を防いだり、システムやハードディスクの負荷に応じて設定を調整することができます。この調整により、OS のより高速な起動や、パフォーマンス向上を実現する事が可能となります。

アンチウイルス

この機能を使用して、コンピュータや記録メディアのウイルス感染が無いか、指定した方法でスキャンすることができます。例えば、友人や家族、職場の同僚から借りたUSBメモリや、CD/DVDなどの感染チェック。インターネットからダウンロードしたソフトの感染チェックにも効果を発揮します。

注意: コンピュータや記録メディアのウイルススキャンは追加的な保護機能です。普段はアイドリングスキャンとウイルスガードが常にバックグラウンドで動作しており、マルウェアの脅威に対して最適な保護を維持します。G Data 製品をインストールする前や、ウイルスガードが無効になっていた間コンピュータにコピーされたウイルスを検出するには、ウイルススキャンを使用してください。

ウイルススキャン

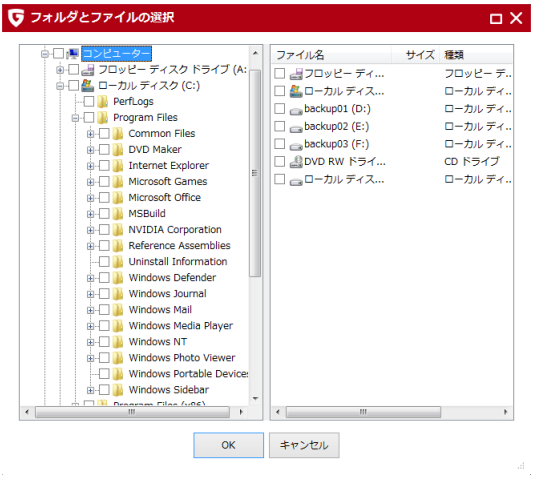
以下の項目からコンピュータやメディアのスキャンを行えます:

コンピュータをスキャン(すべてのローカルドライブ)：ウイルス感染の疑いがある場合など、アイドリングスキャンやスケジュールスキャンとは関係なく、今すぐにコンピュータをスキャンする必要がある時は、ここをクリックします。クリック後は、ただちにスキャンが開始されます。**ウイルススキャンの流れ**の項も参照してください。

メモリとスタートアップをスキャン: 実行中のすべてのプロセスに対して、プログラムファイル および DLL（プログラムライブラリ）をスキャンします。不正プログラムが見つかった場合は、**メモリとスタートアップ領域**から不正プログラムをすぐに除去します。このスキャンは比較的短時間で完了できるため、自動ウイルススキャンなどと一緒に定期的に実行することをお勧めします。

この機能は、データの定期的なウイルススキャンに代わるものではなく、それを補完するものです。

フォルダ/ファイルをスキャン: 選択したドライブ、フォルダ、またはファイルがウイルスに感染していないか調べます。この操作をクリックすると、フォルダとファイルの一覧が表示されます。個々のファイルにターゲットを絞ってスキャンしたり、フォルダ全体のウイルススキャンを行うことができます。
フォルダツリーでは、「+」をクリックするとそのフォルダが展開し、フォルダの内容がファイルビューに表示されます。ウイルススキャンは、チェックボックスにチェックが入っているフォルダまたはファイルに対して、行われます。一部スキャンされないファイルがあるフォルダには、グレーのチェックマークが表示されます。



リムーバブルメディアをスキャン: CD/DVD-ROM、フロッピーディスク、メモリカード、USB メモリなどをスキャンします。この機能を選択すると、コンピュータに接続されているすべてのリムーバブルメディ

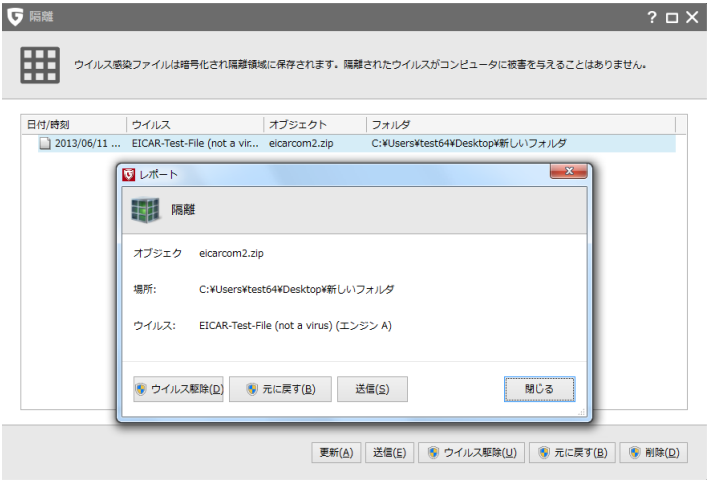
ア（トレイに挿入済みのCD/DVD-ROM、メモリカード、または USB 経由で接続中の外付けハードディスクやUSB メモリ）をスキャンします。ただし、本製品は書き込み不可のメディアに対してウイルス除去できません。スキャン結果にウイルス検出のログが作成されるだけですので、ご注意ください。

ルートキットをスキャン: ルートキットとは、従来のウイルス検出方法では検出が困難な不正プログラムです。この機能を使うと、ハードディスク内の全データすべてをスキャンすることなく、ターゲットをルートキットに絞ってスキャンします。

隔離されたファイル

ウイルス検出時の処理方法の１つに**隔離**という処理方法があります。この操作を行うと、検出されたファイルが他のファイルに危害を及ぼさないように、コンピュータ上に作成された暗号化領域に保存されます。

隔離領域を表示: このボタンをクリックすると、隔離領域が表示されます。



隔離領域に移動したファイルは、検出された時の状態で保存されます。隔離されているファイルには次の操作が可能です:

- **更新**: 隔離情報を更新します。隔離画面を開いてから時間が経過し、他にもウイルスが検出された場合、それらが表示されます。

- **送信**: 感染ファイルを G Data に送信します。感染ファイルが新種の不正ファイルである場合は、その後のワクチン開発に活用されます。ユーザーが送信した情報は匿名情報として処理されます。詳細は、**マルウェア情報イニシアチブ** を参照してください。

  マルウェア情報イニシアチブとは: G Data セキュリティラボでは、G Data 製品をご利用のユーザー様を、コンピュータの安全性を脅かす脅威からから保護するため、保護・対策の研究や分析に絶え間なく励んでいます。 マルウェア研究では、マルウェアに関する情報が多ければ多いほど、効果的な保護メカニズムの開発をいち早く進めることができます。これらの情報をG Data の研究・分析・開発に効率的に取り入れることを可能にするための取り組みが、G Dataマルウェア情報イニシアチブです。 これにより、マルウェアに関するデータをG Dataセキュリティラボに送信することができます。 より多くのユーザー様に参加頂くことで、他のG Data製品をご利用の方々もインターネットをより安全に利用できるようになります。

- **ウイルス駆除**: 感染ファイルから感染部分のみを駆除し、ファイルを元の場所に戻します。場合によっては、駆除はできない場合もあります。

- **元に戻す**: 隔離ファイルを元に戻します。この処理は例外ケースを除き利用しないでください。利用する場合は、コンピュータのネットワーク／インターネット接続を切断し、未感染データをバックアップするなどした上で、実行してください。

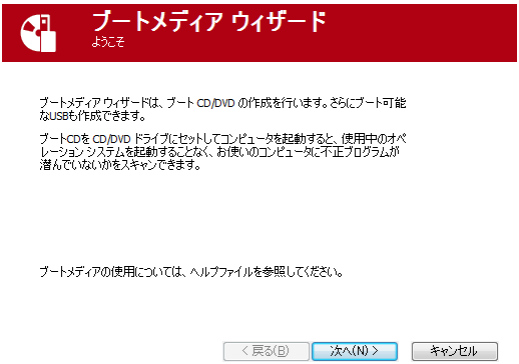
- **削除**: 感染ファイルが不要な場合は、隔離領域から削除できます。

ブートメディア

ブートメディアは、Windows 起動前にスキャンを実行できるブートスキャン機能が搭載しており、本製品のインストール前からコンピュータに感染し、本製品のインストールを妨害する可能性のあるウイルスを駆除するのに役立ちます。詳細は、ブートスキャンの項を参照してください。

ブートメディアを作成する場合は、アンチウイルス画面から**ブートメディアを作成**ボタンをクリックし、ウィザードの指示に従ってください。このウィザードでは、最新の最新のワクチンのダウンロードや、

作成メディア種類（CD/DVD/USB）を選択できます。



復元: G Data トータルプロテクションを使用している場合は、ブートメディアからバックアップイメージをシステムボリュームへ復元、もしくはファイルバックアップを任意のドライブへ復元する事が可能です。復元機能を利用する場合はブートメディアをコンピュータへ挿入し **G Data バックアップ（復元）**を選択してください。

ファイアウォール

ファイアウォールは、外部の不正侵入からコンピュータを防御するため防御する機能で、インターネットやネットワークとコンピュータとの間で送受信されるデータを監視します。

ファイアウォールには以下の3つの領域が存在します:

- ステータス: ステータス領域では、使用中のコンピュータでの一般的なファイアウォール動作状況を確認する事ができます。
- ネットワーク: ネットワーク領域では、コンピュータが接続しているネットワークが表示されます（例: ローカルエリア接続、ワイヤレスネットワーク接続など）。
- ルールセット: ルールセット領域では、ネットワークごとにルールセットを作成し、ファイアウォールの動作を最適化できます。

ファイアウォールは、許可されていないデータの書き込みやダウンロードを検知すると警告を発し、それらのデータ通信を阻止します。

設定: 画面右上にある設定ボタンからは、ファイアウォールの細かな設定を行う設定画面を開くことができます。

ステータス

ステータスでは、ファイアウォールの状態に関する基本情報が項目ごとに表示されます。項目をクリックしてそれぞれの操作を選択すると、機能の切り替えや、設定の編集を行えます。

警告マークの付いた項目の設定が最適化されると、マークは再び緑色のチェックマークに戻ります。

- **セキュリティ**: ファイアウォールは、インターネットに接続したり、コンピュータに悪影響を及ぼすアプリケーションを自己学習していきます。ファイアウォールに関する知識レベルに応じてファイアウォールの設定を変えることも可能です。ユーザーへの確認の頻度を減らしつつ、セキュリティレベルの高い基礎的保護がなされるように設定することもできれば、コンピュータの使用状況に合わせた高水準の保護が得られるように詳細設定することも可能です。ただし、詳細設定を利用するには、ファイアウォールに関する高度な知識が必要です。**セキュリティ**をクリックして**セキュリティを編集**を選択すると、設定画面の 設定 | ファイアウォール | 自動 が開きます。

- **モード**: 作動中のファイアウォール設定を確認できます。設定は、**自動（オートパイロット）**と**手動でルールを作成**のいずれかから選択できます。

  オートパイロット: ファイアウォールがアプリケーションの許可／拒否

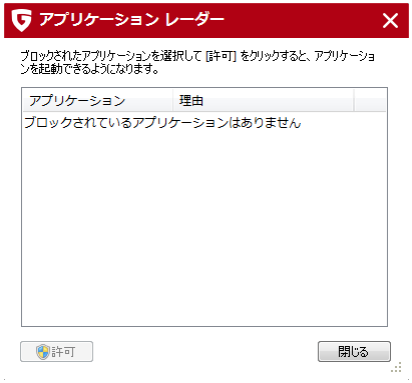
を自動判断で制御し、コンピュータを保護します。この機能は全般的な状況に対応できるため、通常はこの機能を使用することを推奨します。デフォルト設定ではオートパイロットはオンになっています。

詳細設定: ファイアウォールをネットワーク環境に合わせて設定したい場合、あるいは特定のアプリケーションにオートパイロットモードを適用したくない場合には、ルールを手動で作成するように設定を変更できます。この機能の詳細は 設定 | ファイアウォール | 自動 の項を参照してください。

- **ネットワーク**: ファイアウォールが監視しているネットワークの状況を表示します。この機能の詳細は ファイアウォール | ネットワーク の項を参照してください。

- **撃退した攻撃**: コンピュータへの攻撃が検知されると、ファイアウォールはこれをブロックし、ログとして記録します。この項目をクリックし、システムメッセージを表示を選択すると、ブロックした攻撃に関する詳細な情報を見ることができます。

- **アプリケーションレーダー**: アプリケーションレーダーでは、ファイアウォールが起動をブロックしているプログラムを表示できます。ブロックされたアプリケーションのうちネットワーク使用を許可したいものがあれば、そのアプリケーションを選択して **「許可」** をクリックします。



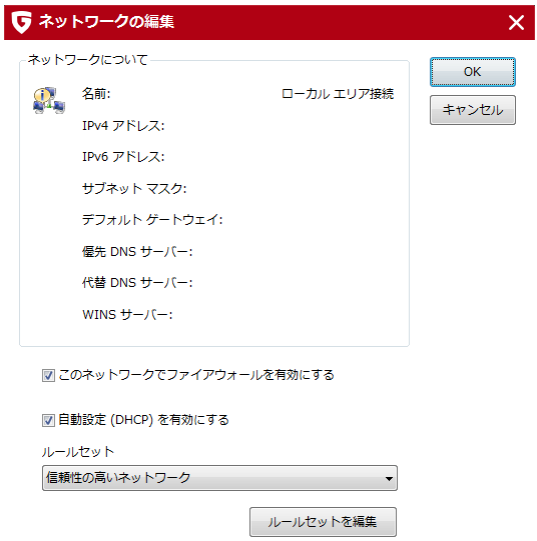
ネットワーク

ネットワークでは、コンピュータが接続しているネットワーク （LAN接続、DTN （ダイヤルアップ接続）など）の一覧、適応されているルールセット、IPアドレスが表示されます。

この画面では使用されているネットワークと、それに使用されているルールセットが一覧表示されます。ネットワーク名の横にあるチェックを外すと、そのネットワークに対するファイアウォールによる保護が解除されます。※特別な理由がない限り、ファイアウォールの保護は解除しないようにしてください。

表示されている設定を確認したり、編集したりするには、対象を選択してダブルクリック（もしくは対象を選択して**「編集」**をクリック）します。

ネットワークの編集
ネットワーク画面で編集を選択すると、選択されたネットワークの各種情報が表示されます:



- **ネットワークについて**: IP アドレス、サブネットマスク、デフォルトゲートウェイ、DNS および WINS サーバーなどのネットワークに関する情報がある場合、それらを表示します。

- **このネットワークでファイアウォールを有効にする**: チェックを外すと、ネットワークに対してファイアウォールを無効にできます。特別な理由がない限り、有効にしておいてください。

- **インターネット接続共有**: インターネットに直接接続している場合、ネットワーク内のすべてのコンピュータに対して、インターネットアクセスの許可または禁止を設定できます。このインターネット接続共有（ICS）は通常、ホームネットワークでのみ有効にできます。

- **自動設定を有効にする（DHCP）**: DHCP（Dynamic Host Configuration Protocol）を使用したネットワークでは、コンピュータを接続すると動的に IP アドレスが割り当てられます。このネットワークに接続している場合は、設定を有効にしてください。

- **ルールセット**: **信頼性の高い**、**信頼性の低い**、または**アクセスを拒否する**ネットワークといった複数のルールセットから選択し、ファイアウォールルールを素早く設定できます。さらに**「ルールセットを編集」**をクリックすると、これらのルールセットを編集して独自のルールを作ることもできます。詳細ついては、**ルールセット**の項を参照してください。

ルールセット

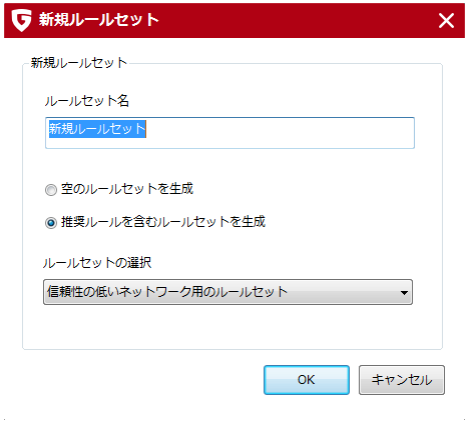
ファイアウォールの細かいルール郡から構成されているルールのまとまりをルールセットといいます。ルールセット領域では、それぞれのネットワークに応じた固有のルールを作成できます。作成されたルールセットは、ルールセット領域にすべて表示されます。

本製品にプリセットされているルールセットには、**アクセスを拒否するネットワーク**、**インターネットに直接接続**、**信頼性の低いネットワーク**、**信頼性の高いネットワーク**があります。それぞれのルールセットの内容を確認や修正するには、ルールセットを選択して**「編集」**を押します。新規ルールを作成するには、**「新規作成」**のボタンを押し、ダイアログに沿ってルールを作成してください。

メモ: ユーザーによって作成されたルールセットは削除できますが、本製品に前もって設定されているルールセットは削除できません。

新規作成
ネットワークごとに異なる設定のルールセットを割り当てる事で、ファイアウォールは様々なセキュリティレベルのネットワークに対応できます。例えば、一般的に、ホームネットワークに接続している場合は、インターネットに直接接続している場合よりも緩めのルールで十分効果を発揮します。

ルールセットは自分で作成する事も可能です。新規ルールを作成するには、**「新規作成」**のボタンを押してください。
次に表示される、以下のダイアログに沿ってルールを作成してください:



- **ルールセット名**: ルールセットの名前を入力します。
- **空のルールセットを生成**: 空のルールセットを作成しておいて、ルールを自身で定義して追加します。
- **推奨ルールを含むルールセットを生成**: G Data のプリセットルールの**信頼性の高いネットワーク**、**信頼性の低いネットワーク**、**アクセスを拒否するネットワーク**から選択してルールを作成します。作成されたルールセットは、必要に応じて後からカスタムできます。

ファイアウォールには、ネットワークの種類ごとに以下のデフォルトルールセットが用意されています:

- **インターネットに直接接続**: インターネットに直接接続している環境用のルールセットです。
- **信頼性の低いネットワーク**: ダイヤルアップネットワークやその他のインターネット接続するオープンネットワーク用のルールセットです。
- **信頼性の高いネットワーク**: ホームネットワークや企業ネットワークなどの信頼できるネットワーク用のルールセットです。
- **アクセスを拒否するネットワーク**: あるネットワークへの接続を一時的または常時ブロックするためのルールセットです。この設定は、セキュリティのレベルが不明なネットワーク （例: 他社の企業ネットワーク、公共ネットワークなど）に接続する時に適用してください。

新規作成されたルールセットは、ルールセット領域に表示されます。作成したルールセットを変更するには、そのルールセットを選択して**「編集」**を押してください。設定 | ファイアウォール | その他 の**デフォルトで使用するウィザードの種類**で定義されている方法でルールセットをを編集できます。

新規ルールの作成方法は、ルールウィザード もしくは 拡張ルールセットエディタ の項を参照してください。

オートパイロットを使用していない場合、新規ルールをポップアップで表示されるアラートからも作成できます。詳細は ファイアウォールアラート の項を参照してください。

ルールウィザード
ルールウィザードは、既存のルールセットに特定のルールを追加したり、既存のルールを編集する際に、ユーザーをサポートするウィザード形式の設定アシスタントです。ファイアウォール上級者以外は、**拡張ルールセットエディタ**よりも**ルールウィザード**を利用することをお勧めします。

ルールウィザードを使用すると、選択したルールセットに含まれるルールを簡単に編集できます。
ネットワークごとに適用したルールセットの種類によって、アプリケーションは遮断されたり、許可されたりします。例えば、ホームネットワークでネットワーク接続を許可する一方で、ダイヤルアップ接続では拒否するといった設定も可能です。

ルールウィザードでは次の基礎ルールを選択できます:

- **アプリケーションを許可/拒否**: インストールされているアプリケーションを選択し、ルールセットで指定したネットワークへのアクセスを許可／拒否します。目的のアプリケーションのある場所を示す文字列（**パス**）を選択して、**接続の方向**でそのプログラムにインバウンド接続（着信接続）、アウトバウンド接続（発信接続）のどちらを許可するか、あるいはイン／アウトバウンド接続の両方を許可するかどうかを設定します。例えば、音楽再生ソフトの場合では、次のような利用ができます。

  アウトバウンド接続を拒否して、ユーザーの音楽嗜好データを自動送信するのを防止
  インバウンド接続を拒否して、プログラムの自動更新を遮断

- **ネットワークサービスを許可/拒否**: **ポート**とは、外部とデータを入出力するため、アプリケーションによって使用されるネットワークアドレスの一部です。例えば、ウェブページの閲覧ではポート80、メール送信にはポート25、メールの受信にはポート110が割り当てられています。ファイアウォールを使用しない場合には、すべてのポートが開放状態になっているので、外部の第三者から攻撃を仕掛けられる可能性があります。ルールウィザードを使用すると、特定のアプリケーションに必要なポートのみ許可し、その他のポートは遮断します。

- **ファイルおよびプリンタ共有を許可/拒否**: 主にNetBIOSに関する設定です。NetBIOSとはLANでネットワークを利用する際の通信規約で、TCP/IPプロトコルなどを使用せずに、コンピュータ間で直接ファイルやプリンタを共有するのに利用されています。これは、一般的なホームネットワークではほぼ不要ですが、ハッカーが NetBIOS を使ってコンピュータを攻撃する可能性もあるので、信頼性の低いネットワークに対しては共有を拒否してください。

- **ドメインサービスを許可/拒否**: ドメインはあるネットワーク内にあるコンピュータを整理して一覧できるようにするためのもので、ネットワークに接続しているコンピュータを1か所で管理できるように割り当てられています。ドメインサービスを許可（もしくは拒否）します。信頼できないネットワークでのドメインサービスの共有は拒否してください。

- **インターネット接続共有を許可/拒否**: インターネットに直接接続している場合、ネットワーク内のすべてのコンピュータに対して、インターネットアクセスの許可または禁止を設定します。このインターネット接続共有（ICS）は通常、ホームネットワークでのみ有効にするものです。

- **VPNサービスを許可/拒否**: VPNはVirtual Private Networkの略で、別ネットワークにあるコンピュータ同士を接続し、あたかも直接接続しているかのように動作させることのできる技術です。VPN接続を利用している場合は、この設定を許可する必要があります。

- **拡張ルールセットエディタへ切換え（エキスパートモード）**：ファイアウォールのルールウィザード（ルールセットの作成モード）から拡張ルールセットエディタへ切換えます。

拡張ルールセットエディタ

ネットワークセキュリティに関してある程度の知識があるユーザーは、拡張ルールセットエディタを使ってルールセットを更に詳細に設定できます。このエディタでは、ルールウィザードでは難しい高度な設定が可能です。

拡張ルールセットエディタでは次の設定ができます:

- **名前**: 選択したルールセットの名前を変更できます。ルールセットはこの名前で**ルールセット**領域に表示され、ファイアウォールが識別したネットワークに結び付けられます。

- **ステルスモード**: ステルスモードを使用すると、コンピュータで使用しているポートの確認に対して応答せず、ハッカーなどがシステム情報を取得するのを困難にします。

- **ルールにないアクセスが検知された場合の操作**: ネットワークのアクセスをすべて許可／拒否するか、あるいはユーザーへの確認で決めるかを設定できます。ファイアウォールの学習機能で個々のアプリケーションに専用ルールを設定している場合は、そのルールが適用されます。

- **アダプティブモード**: フィードバックチャネル技術を使用するアプリケーション（FTPや各種オンラインゲームなど）をサポートします。この種のアプリケーションはリモートコンピュータに一旦接続し、その後、リモートコンピュータがユーザーのアプリケーションに「逆接続」する

フィードバックチャネルを確保します。アダプティブモードを有効にしておくと、ファイアウォールがこのフィードバックチャネルを検出し、確認を求めることなく接続を許可します。

ルール
ルール領域には、ルールセットに含まれるに細かなルールが登録されています。

ルールセットは以下の3種類の方式で作成されます。:

- ルールウィザード
- 拡張ルールセットエディタ （エディタ内の**新規作成**ボタンを押して新しいルールを作成できます）
- アラート （アラートダイアログ経由でルールが作成された場合は、エディタ内のコメント欄に「アラートにより作成」と表記されます）

これらの方法で作成されたルールセットには、それぞれ独自のルールが含まれています。

ファイアウォールルールは、一部が階層構造でまとめられているため、場合によってはルールの**ランク順**に注意する必要があります。例えば、ポートを開放しているにもかかわらず、そのポートを利用しているアプリケーションが遮断される可能性があります。このような場合は、ルールのランク順を変更するとアクセスが許可されるようになります。ランク順を変更するには、目的のルールをマウスで選択して **ランク**の欄の矢印ボタンでリストの上位または下位へ移動してください。

拡張ルールセットエディタで**「新規作成」**から新規ルールを作成したり、**「編集」**ボタンから既存ルールを変更すると、**ルールを編集**ダイアログが表示されます。

このダイアログでは、以下の項目を設定できます:

- **名前**: デフォルトルールおよび自動的に作成されたルールの場合、アプリケーション名が入ります。名前は自由に変更できます。
- **有効なルール**: ルールの有効／無効を切り替えます。ルールを無効にするには、チェックを外します。ルール自体の削除はされません。
- **コメント**: ルールを作成した方法が表示されます。ルールセットに対するデフォルトルールには**デフォルトルール**、アラートから作成したルールには**アラートにより作成**と自動的に入力され、ユーザーが詳細設定ダイアログで作成したルールの場合にはユーザーが自分でコメントを入力できます。
- **接続の方向**: ルールをインバウンド接続（着信接続）とアウトバウンド接続（発信接続）のどちらに適用するかを指定します。
- **アクセス**: ルールセットに関連するプログラムに対してアクセスを許可するかどうかを設定します。

- **プロトコル**: アクセスを許可または禁止する接続プロトコル を選択できます。このとき、プロトコルを原則として停止または許可する、またはプロトコルの使用を1つのアプリケーションまたは複数のアプリケーションと組み合わせる（**アプリケーション割当て**）ことができます。同様に、許可するポートとブロックするポートを**「インターネットサービス割当て」**から厳密に定義できます。

- **時間**: ネットワークリソースへのアクセス時間を設定できます。例えば、アクセス許可を業務時間内に限定して、それ以外の時間はアクセスできないように設定できます。

- **IP アドレス範囲**: 固定 IP アドレスを持ったネットワークでは、IP アドレス範囲を限定して使用方法も可能です。IP アドレス範囲を厳密に定義すれば、ハッカーから攻撃を受ける危険性を大幅に低減できます。

フィルタリング

フィルタリング機能は、お子様がコンピュータを使用する際などに、ウェブサイトを一定の基準で評価判別して排除したり、コンピュータの利用時間に制限をかける機能です。

ユーザーでコンピュータに登録されているユーザーアカウントを選択し、以下の項目からそれぞれに適した設定を行ってください。Windows の新規ユーザーアカウント（例:子供用アカウントなど）を作成したい場合は、**新規ユーザー**ボタンから作成する事ができます。

- **このユーザーのフィルタリング**: ここでフィルタリングのオン/オフを切り替えられます。
- **禁止するコンテンツ**: **編集**をクリックするとダイアログが開き、指定したユーザーに対してブロックするウェブコンテンツを指定できます。
- **許可するコンテンツ**: **編集**をクリックするとダイアログが開き、指定したユーザーに対して許可するウェブコンテンツを指定できます。
- **インターネット利用時間の監視**: **編集**をクリックするとダイアログが開き、指定したユーザーに対してどれくらいの期間（またはどの時間帯）インターネットの接続を許可するかを設定できます。

- **コンピュータ利用時間の監視**: 編集をクリックするとダイアログが開き、指定したユーザーに対してどれくらいの期間（またはどの時間帯）インタコンピュータの使用を許可するかを設定できます。

設定: フィルタリング機能のログに関する動作を設定できます。

新規ユーザー

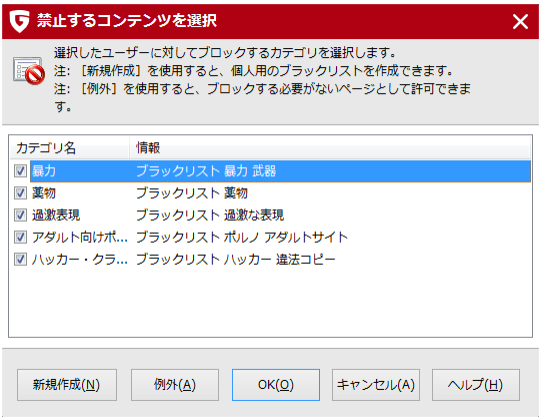
「新規ユーザー」をクリックすると、ダイアログが開きます。ここでユーザー名とパスワードを入力してください。

安全のため、パスワードは、『8文字以上（大文字と小文字、数字を含む）』で構成するようにしてください。

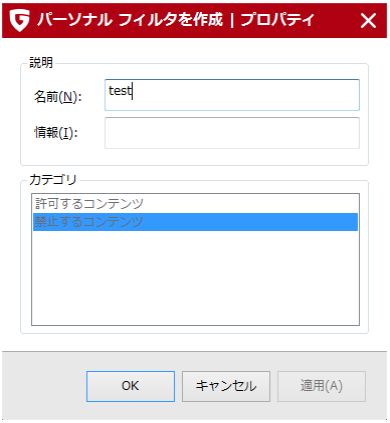
各項目を入力した後に「作成」をクリックすると**Windows ユーザーアカウント**が作成され、ステータス領域の**ユーザー**に新しく追加したユーザー名が表示されるようになります。Windows起動時に作成したユーザー名でログインすると、そのユーザー用に設定したフィルタリングの設定が有効になります。ユーザー用のフィルタリング設定を変更したり確認するには、**禁止するコンテンツ**、**許可するコンテンツ**、**インターネット利用時間の監視**、**コンピュータ利用時間の監視**選択し「編集」をクリックしてください。

禁止するコンテンツ

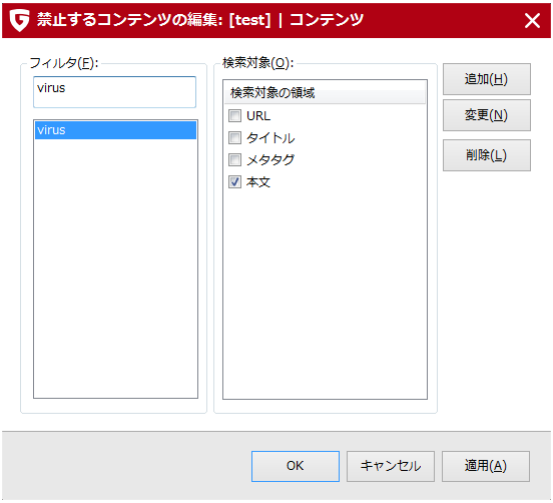
ダイアログ画面で、ユーザーが閲覧することを禁止するコンテンツを設定します。禁止するコンテンツを有効にするには、禁止したいカテゴリにチェックを入れます。**「OK」**をクリックすると、**禁止する基準**を満たすウェブサイトを表示できなくなります。



「新規作成」をクリックするとダイアログ画面が開き、禁止するコンテンツを独自に作成できます。コンテンツを作成するには、**パーソナルフィルタを作成**の画面で、**名前**の欄に入力し（必要であれば**情報**欄に説明を入力して）、**「OK」**をクリックしてください。



「OK」をクリックすると、**禁止するコンテンツの編集**の画面が開きます。



フィルタの欄に表示を禁止するキーワードを入力し、**検索対象**でキーワードを検索する範囲を選択してください。

検索対象は以下の項目から選択できます:

- URL: ウェブアドレス内の文字列を検索します。例えば、www.chatcity.co.jp、www.crazychat.co.jp などのサイトを禁止したい場合、**フィルタ**欄に 「chat」 と入力し、URLにチェックを入れて**「追加」**をクリックします。この設定が有効になると、URLに 「chat」 という文字列が含まれているページがすべて閲覧できなくなります。

- **タイトル**: ウェブサイトのタイトルの文字列を検索します。ここでいうタイトルとは、ウェブページを**ブックマーク**に追加する時に表示されるウェブサイトに付与されている名前です。例えば、Chat City Japan、Teenage Chat などのサイトを禁止したい場合、**フィルタ**欄に 「chat」 と入力し、**タイトル**にチェックを入れて**「追加」**をクリックします。この設定が有効になると、**タイトル**に 「chat」 という文字列を使用しているページはすべて閲覧できなくなります。

- **メタタグ**: **メタタグ**（検索エンジンによる検索結果を上げるために利用されるタグです））に記載されている文字列を検索します。例えば、メタタグ内のどこかに文字列「chat」が記述されているページを閲覧禁止にするには、**フィルタ**欄に「chat」と入力し、**メタタグ**にチェックを入れ

て**「追加」**をクリックします。この設定が有効になると、メタタグ内に「chat」 という文字列が含まれているページがすべて閲覧できなくなります。

- **本文**: **フィルタ**欄に「chat」と入力し、次に**本文**にチェックを入れて、**「追加」**をクリックします。この設定が有効になると、本文内に 「chat」 という文字列が含まれているページがすべて閲覧できなくなります。

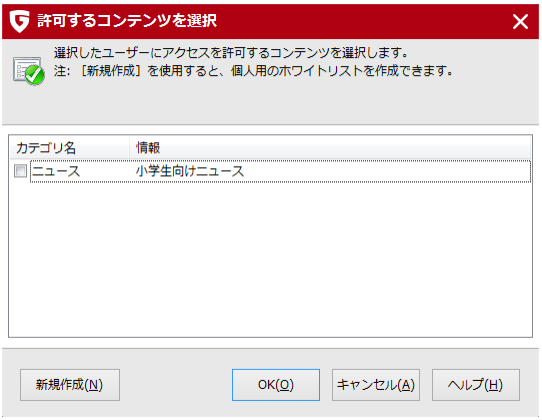
通常利用されるキーワードを**フィルタ**に設定すると、無害なウェブページを閲覧できなくなることもあります。例えば、禁止キーワードに「cash」を登録すると、「Cashew」という文字列を含むウェブページの閲覧も禁止されかねません。

フィルタに引っ掛かりやすいウェブページを許可するには、**例外**機能を使って例外扱いします。例外を追加するには、まず作成したブラックリストを選択し、**「例外」**をクリックします。例外リストの画面が開くので、上述の例であれば、「Cashew」をフィルタに入力して、**「追加」**をクリックします。

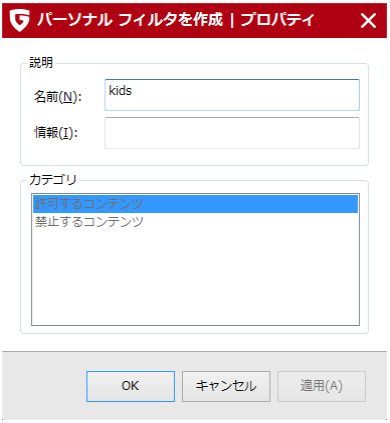
> 禁止するコンテンツで追加したフィルタは、**パーソナルフィルタ**領域では、種類の列に**ブラックリスト**と表示されます。作成済みフィルタは、自由に編集したり削除できます。詳細については、パーソナルフィルタの項を参照してください。

許可するコンテンツ

ダイアログ画面で、ユーザーが閲覧することを許可するコンテンツを設定します。許可するコンテンツを有効にするには、許可したいカテゴリにチェックを入れます。「OK」をクリックすると、**許可するコンテンツの編集**で設定したウェブサイトの表示が許可されます。



「**新規作成**」をクリックするとダイアログ画面が開き、許可するコンテンツを独自に作成できます。コンテンツを作成するには、**パーソナルフィルタを作成**の画面で、**名前**の欄に入力し（必要であれば**情報**欄に説明を入力して）、「OK」をクリックしてください。



「OK」をクリックすると、**許可するコンテンツの編集**の画面が開きます。

次に、**フィルタ**の欄に許可する**ドメイン名の一部**入力します。（例：*nickjapan*）。**説明**の欄には、ウェブページの内容 （前述の例の場合、「*nickjapan*: 子供向けウェブページ」など）を入力します。**サイトへのリンク**の欄には、ウェブサイトの正確なアドレス（例: www.nickjapan.com）を入力します。**説明**と**サイトへのリンク**に情報を入力すると、ユーザーが禁止されたサイトにアクセスしようとした場合に、許可するリストに登録されたウェブサイトがブラウザ上に表示されます。すべての情報を入力して**「追加」**をクリックすると、情報が許可するコンテンツに登録されます。

フィルタやドメインの入力が間違っているとウェブサイトの表示ができませんのでご注意ください。また、説明はアクセス可能なインターネットサイトのリストにリンク名として表示されますので、お子様などの使用者を想定して設定してください。

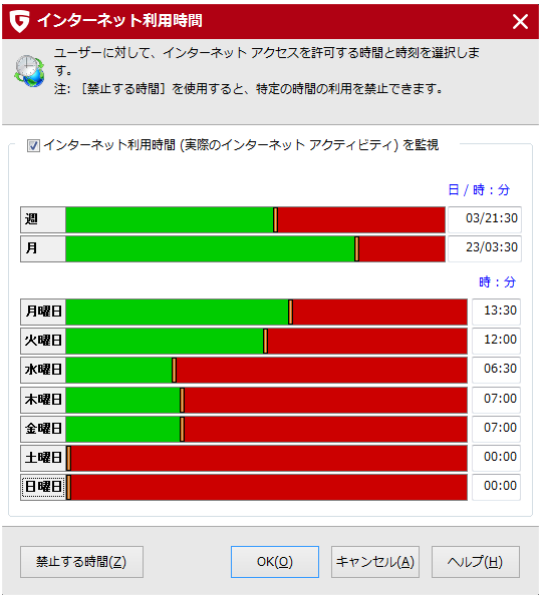
フィルタはドメイン名に含まれる文字を検索します。入力する文字によって表示基準の厳密さを調整する事も可能です。

許可するコンテンツで追加したフィルタは、**パーソナルフィルタ**領域では、種類の列に**ホワイトリスト**と表示されます。作成済みフィルタは、自由に編集したり削除できます。詳細については、パーソナル

フィルタの項を参照してください。

インターネット利用時間の監視

ユーザーのインターネット利用時間を設定します。まずは、ステータス領域でユーザーを選択し、次に**インターネット利用時間の監視**、**編集**をクリックします。**インターネット利用時間**の設定画面が現れるので、そこで**インターネット利用時間を監視**にチェックを入れます。許可する時間は、月次、週次、曜日ごとに設定できます。許可する時間は、**日 / 時：分** の欄に入力するか、マウスを使ってバーをスライドさせて設定します。例えば、**「04 / 20：05」** と入力すると、インターネットの利用時間は「4 日間、20 時間と 5 分」となります。



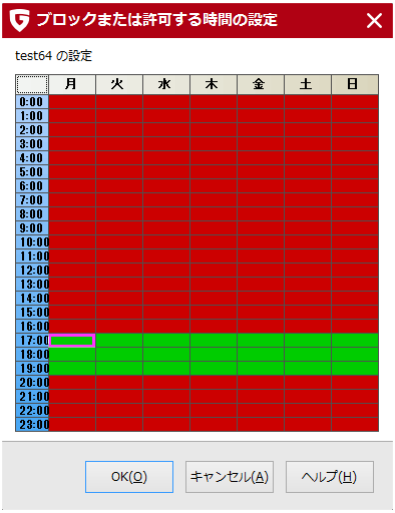
インターネット利用時間の設定では、常に最小値が適用されます。例えば、1 か月の時間制限を 4 日間と設定する一方で 1 週間の時間制限を 5 日間と設定した場合、ソフトウェアはこのユーザーのインターネット利用時間を自動的に 4 日間に制限します。

ユーザーが許可された制限時間を超えてインターネットにアクセスしようとすると、ブラウザに利用制限時間を超過したことを知らせるメッセージが表示されます。

禁止する時間

「禁止する時間」をクリックしてダイアログを呼び出し、インターネットにアクセスできる時間の量的制限に加えて、週のうちの特定の時間帯にインターネットにアクセスできないように設定できます。

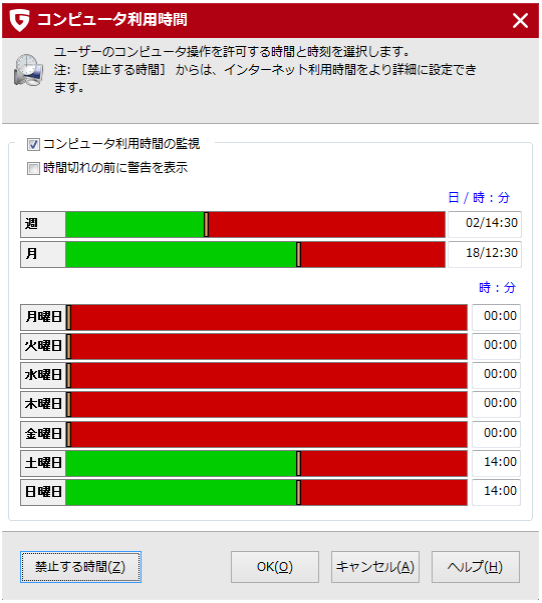
禁止する時間帯は赤色、許可する時間帯は緑色で表示されます。 許可または禁止する時間を指定するには、マウスで時間帯を選択し、マウスポインタの横に表示されるコンテキストメニューで**許可する時間**もしくは**禁止する時間**のいずれかを選択します。ユーザーが禁止時間にインターネットにアクセスしようとすると、ブラウザに利用できない時間帯である事を知らせるメッセージを表示されます。



コンピュータ利用時間の監視

ユーザーのコンピュータ利用時間を設定します。まずは、ステータス領域でユーザーを選択し、次に**コンピュータ利用時間の監視、編集**をクリックします。**コンピュータ利用時間**の設定画面が現れるので、そこで**コンピュータ利用時間の監視**にチェックを入れます。許可する時間は、月次、週次、曜日ごとに設定できます。許可する時間は、**日 / 時 : 分** の欄に入力するか、マウスを使ってバーをスライドさせて設定します。例えば、**「04 / 20 : 05」** と入力すると、インターネットの利用時間は「4 日間、20 時間と 5 分」となります。

時間切れの前に警告を表示にチェックをいれると、コンピュータが自動的にシャットダウンされる前に、ユーザーにその旨を知らせることができます。コンピュータが事前の警告なしにシャットダウンされると、データの消失などの原因になります。

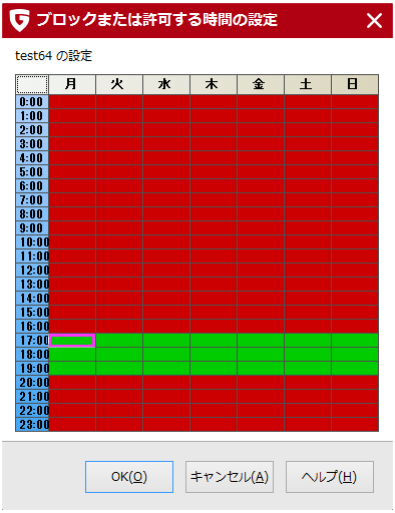


Note: コンピュータ利用時間の設定では、常に最小値が適用されます。例えば、1 か月の時間制限を 4 日間と設定する一方で 1 週間の時間制限を 5 日間と設定した場合、ソフトウェアはこのユーザーのコンピュータ利用時間を自動的に 4 日間に制限します。

禁止する時間

「禁止する時間」をクリックしてダイアログを呼び出し、コンピュータを使用できる時間の量的制限に加えて、週のうちの特定の時間帯にコンピュータを使用できないように設定できます。

禁止する時間帯は赤色、許可する時間帯は緑色で表示されます。 許可または禁止する時間を指定するには、マウスで時間帯を選択し、マウスポインタの横に表示されるコンテキストメニューで**許可する時間**もしくは**禁止する時間**のいずれかを選択します。



パーソナルフィルタ

自分で作成した**許可するコンテンツ（ホワイトリスト）**と**禁止するコンテンツ（ブラックリスト）**の新規作成や変更ができます。

パーソナルフィルタには以下の種類が利用できます:

- **許可するコンテンツ（ホワイトリスト）**：選択したユーザーに対してホワイトリストを選択すると、このユーザーはそのホワイトリストに登録されているウェブページにしかアクセスできません。管理者はホワイトリストをそれぞれのユーザーにカスタマイズしたり、既存のホワイトリストからそれぞれのユーザーに合ったリストを選択できます。ホワイトリストは、特に幼少の子供へのインターネットアクセス制限を行いたい場合に有効で、教育上有益なウェブページのみ利用させるために役立ちます。

- **禁止するコンテンツ（ブラックリスト）**：ブラックリストはユーザーに特定サイトへのアクセスを禁止します。ブラックリストで指定した以外のコンテンツには自由にアクセスできます。例えば、ブラックリストで指定したサイトと類似したコンテンツを含むサイトにはアクセスできます。もし制限をより確実にしたい場合は、URL 以外の別要素を禁止項目に含むか、ホワイトリストをご利用ください。

各リストの編集には以下のボタンを使用できます:

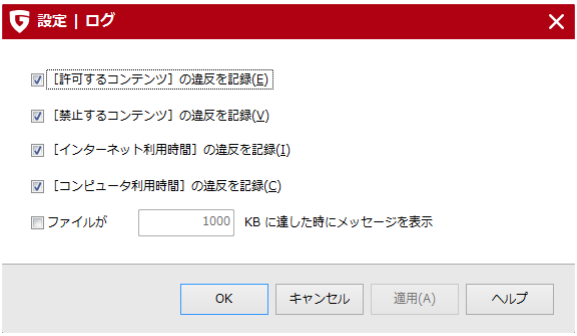
- **削除**: 選択したリストを削除します。

- **新規作成**: ブラックリストまたはホワイトリストを新規作成します。詳細は、**禁止するコンテンツ** および **許可するコンテンツ** の項を参照してください。

- **編集**: 既存リストの内容を変更します。

設定|ログ

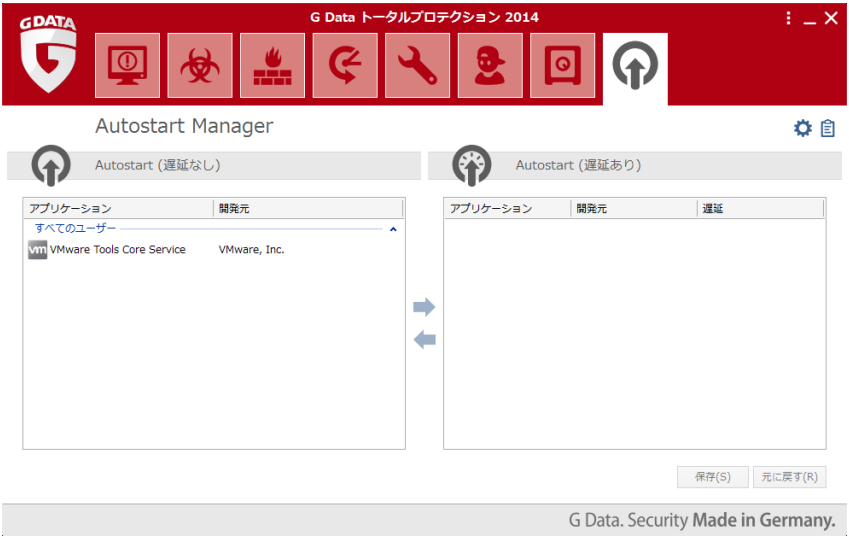
この画面では、ログ取得に関する基本設定を変更でき、各違反ごとにログを記録するかどうかを設定できます。ログは各ユーザーごとに保存され、ログ画面でユーザーごとのログを確認できます。



使用環境によっては、ログファイルの容量が非常に大きくなります。ログファイルがディスク容量を圧迫するようであれば、**ファイルが__KBに達したときにメッセージを表示**にチェックを入れて、適当な数値を入力してください。ログのファイルサイズが設定された数値に到達すると、ユーザーに通知します。ログを削除したい場合は、ログ領域の**「ログを削除」**から削除できます。

オートスタートマネージャー

オートスタートマネージャーは、Windows 起動時に自動起動するプログラムを管理するモジュールです。通常、自動起動プログラムは Windows のスタートアップにロードされますが、オートマネージャーを使うと、任意の自動起動プログラムの起動を指定した時間で遅らせて起動でき、Windows の起動を高速化できます。



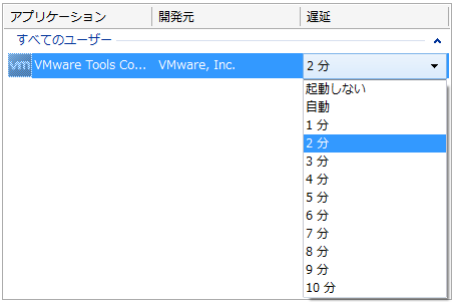
オートスタートマネージャーを初めて開くと、画面左側にコンピュータにインストール済みの自動起動プログラムの一覧が表示されます。これらは Widows の起動直後に起動されるため、起動所要時間に直接の影響を及ぼします。

自動起動プログラムを遅らせて起動するには、まず対象のプログラムを選択して矢印アイコンをクリックし、右側の領域**スタートアップ（遅延あり）**に移動させます。

遅らせて起動している自動起動プログラムを再び遅延なしで起動するには、対象のプログラムを選択して矢印アイコンをクリックし、左側の領域**スタートアップ（遅延なし）**に移動します。

遅延の設定

オートスタート（遅延あり）のプログラムは、起動を指定した時間で遅らせて起動できます。遅延時間を変更するには、対象プログラムの**遅延カラム**上でクリックします。プルダウン表示されるオプションから、選択してください。

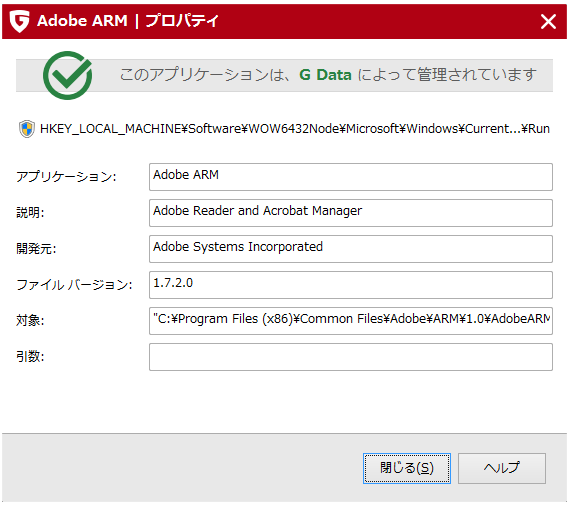


以下のオプションが選択できます。

- **起動しない**: Windows の次回起動時から起動されなくなります。
- **1 - 10 分**: ここで指定する時間に準じてアプリケーションが起動されます。
- **自動**: CPUと保存領域の負荷状況を判断しながら自動起動します。

プロパティ

オートスタートマネージャーで表示されるプログラム上でダブルクリックすると、対象の自動起動プログラムのプロパティを表示させることができます。



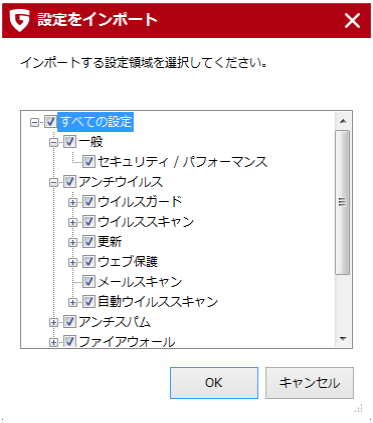
設定

設定領域では、本製品に搭載されている機能の設定項目を確認したり変更ができます。設定画面の左上アイコンからは、次の機能が利用できます。

設定をエクスポート: 設定ファイルを作成します。複数のコンピュータに製品をインストールして共通の設定でコンピュータを管理する場合、この機能を利用すると便利です。

設定をインポート: ここから設定ファイルをインポートします。インポートを実行するには、ここをクリックし、設定ファイルを指定してインポートを実行します。設定のインポートは、チェックマークを操作して、設定をインポートするモジュールや各モジュールの項目を選択します。

設定をリセット: 何らか理由で現在の設定をデフォルトの状態に戻したい場合は、このアイコンから簡単にリセットできます。リセットは、インポートの操作と同じ様にモジュールやモジュールに含まれる設定項目単位でリセットすることが可能です。



一般

セキュリティ/パフォーマンス
ここでは、コンピュータの性能に応じて簡易的にセキュリティ設定を最適化できます。下のメーターでは、それぞれの設定が及ぼすパフォーマンスやセキュリティ性能への影響を確認できます。まず簡単に動作の調整を行いたい、という場合にはこの機能を使用すると便利です。

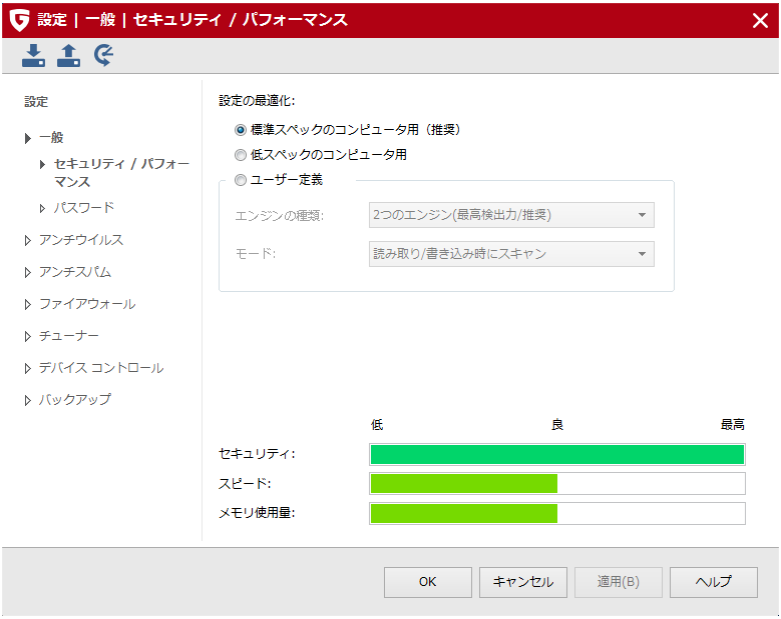
- **標準スペックのコンピュータ用 (推奨)**: 2種類のエンジンを使い、最適な保護を提供します。この設定では、ウイルスガード（オンアクセス機能）はすべての読み取り/書き込みアクセスをチェックします。

  エンジン: G Data には、2種類のエンジンが搭載されています。コンピュータの保護レベルを最適に保つためにも、この設定を利用することをお勧めします。

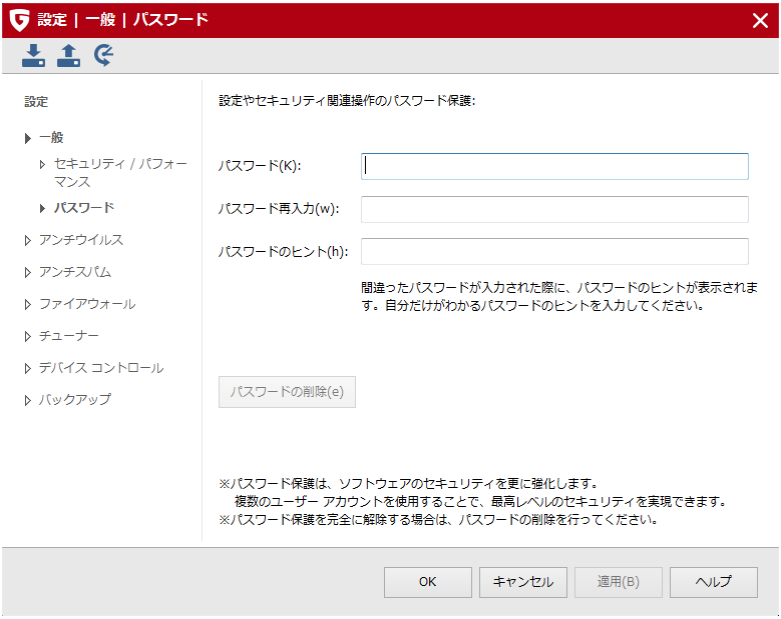
- **低スペックのコンピュータ用**: 低スペックのコンピュータでは、コンピュータの処理速度が遅くなることがあります。その場合は、1つのエンジンのみを利用することで、パフォーマンス低下を回避することができます。この設定では、ウイルスガード（オンアクセス機能）は実行アクセスのみをチェックします。

  市販の大部分のウイルス対策ソフトには1種類のみのエンジンが搭載されていることからも、1種類のエンジンのみで稼動したとしても、セキュリティ保護レベルが大幅に低下することはありません。

- **ユーザー定義**: エンジンとウイルスガード（オンアクセス機能）の設定をお好みでカスタマイズできます。**モード**では、**無効（非推奨）**以外のオプションを選択してください。**無効（非推奨）**を選択すると、セキュリティレベルが著しく低下するので、推奨されません。


設定 | 一般 | セキュリティ / パフォーマンス
設定
一般
セキュリティ / パフォーマンス
パスワード
アンチウイルス
アンチスパム
ファイアウォール
チューナー
デバイス コントロール
バックアップ
設定の最適化:
標準スペックのコンピュータ用（推奨）
低スペックのコンピュータ用
ユーザー定義
エンジンの種類:
2つのエンジン(最高検出力/推奨)
モード:
読み取り/書き込み時にスキャン
低
良
最高
セキュリティ:
スピード:
メモリ使用量:
OK
キャンセル
適用(B)
ヘルプ

パスワード
本製品では、設定にパスワード保護を行うことができます。パスワード設定により、別のユーザーが本製品の設定を不正操作することを防ぐことができます。



パスワードを設定するには、設定画面の左側の領域で**パスワード**を選択し、画面右側の**パスワード**と**パスワードの再入力**の2箇所のフィールドで、パスワード入力を行います。**パスワードのヒント**では、万一パスワードを忘れた際に表示するヒントを入力します。
パスワードの設定後に各設定を変更したい場合は、設定画面の右下に表示されるボタンをクリックし、パスワードを入力してください。

> **メモ**: パスワードのヒントは、間違ったパスワードが入力された場合に表示されます。パスワードを設定した本人だけがわかるヒントを指定してください。

> **メモ**: パスワード保護は、セキュリティレベルをアップさせるための有効な手段ですが、1台のコンピュータを複数ユーザーで共同利用する環境では、各ユーザーに専用のアカウントを作成することをお勧めします。これにより、管理者権限を持つユーザーのみが変更することが許

可され、制限された権限を持つコンピュータの利用者は変更ができないようになります。

メモ: コンピュータの各ユーザーにユーザーアカウントをセットアップしたなどして、パスワードが不要になった場合は、**パスワードの削除**のボタンからパスワードを削除できます。

注意: パスワードの設定後は、**パスワードの削除**を行わない限り、設定変更を行いたい場合に毎回パスワード入力が必要になりますのでご注意ください。

アンチウイルス

リアルタイム保護

本製品では、リアルタイム保護を継続的に提供するウイルスガード（オンアクセススキャン）機能を提供しています。この機能は、コンピュータ上で行われる読み取り/書き込み処理を常時チェックし、 マルウェアの実行や拡散を未然に防ぎます。ウイルスガードは、アンチウイルス機能で最も重要な機能の1つです。通常は、この機能は無効にしないようにしてください。

リアルタイム保護で利用できる項目です。

- **有効（推奨）**: このチェックマークボックスから、ウイルスガードのオン/オフを切換えきます。

- **エンジンの種類**: ウイルススキャンに使用するエンジンを選択します。G Dataには、2 種類の高性能ウイルス検索エンジンを搭載し、世界最高レベルのウイルス検出率を実現しています。通常は、**2つのエンジン（最高検出力/推奨）**に設定してください。もしコンピュータの処理速度に問題がある場合は、1種類のエンジンのみを使用することにより、パフォーマンスを改善することもできます。

- **感染したファイル**: 感染ファイルが検出された場合の処理方法を設定します。デフォルト設定では、感染ファイルの処理方法をユーザーに確認します。なお、データを最高セキュリティで保護するには、**ウイルス駆除（不可能な場合は隔離）**に設定します。

- **感染したアーカイブ**: アーカイブファイル（RAR、ZIP または PST などの拡張子を持つファイル）を通常ファイルと別扱いするかどうかを設定します。なお、隔離されたアーカイブファイルは、元に戻す場合に破損する場合があります。感染したアーカイブは、**ユーザーの操作を待つ**を選択し、検出の度に処理方法をユーザーに選択させることをお勧めします。

- **ふるまい検知**: コンピュータ上のWindows のレジストリやHOSTSファイルへのアクセスやネットワークアクティビティを監視します。これにより、通常のウイルススキャンで検出できなかった不正プログラムを検出します。

例外
ウイルスガードによるスキャンが不要なドライブ、ファイル、およびフォルダをスキャン対象から除外する設定を行います。

例外を設定するには、以下の手順に沿って行います。

1 **[例外]** を選択します。

2 **ウイルスガード用の例外設定**のダイアログ画面で、**[新規作成]** を選択します。

3 次の**例外設定**の画面で、除外対象を**ドライブ、フォルダ、ファイル**を選択できます。

4 ドライブまたはフォルダを指定する場合は、対象を入力欄に直接入力、もしくは、「 ... 」をクリックして対象を指定します。ファイルを指定するには、完全なファイル名もしくはワイルドカードを含むファイル名を設定します。

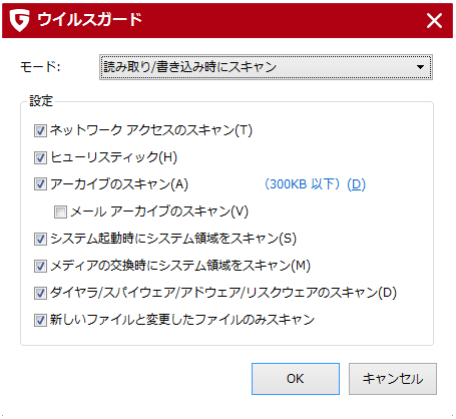
メモ: ワイルドカードの機能について

- 疑問符（?）：任意の1文字を表すためのワイルドカード
- アスタリスク（*）：文字列全体を表すためのワイルドカード

例: 拡張子「.sav」のファイルをすべて対象に設定するには、「*.sav」と入力します。連続性のある名前のファイル（text1.doc、text2.doc、text3.doc など）などを保護するには、「text?.doc」と入力します。

この手順を繰り返して例外設定行うことにより、自身の環境に適したウイルスガード用例外をカスタマイズできます。また、作成した例外設定は、**ウイルスガード用の例外設定**画面の**例外**で表示され、編集や削除の操作は、それぞれ **[編集]** と **[削除]** から可能です。

詳細設定
[詳細設定] からは、ウイルスガードによるスキャンの設定確認や変更ができます。



以下の項目を設定できます。

- **モード**: スキャンするタイミングを設定します。設定は、**読み取り/書き込み時にスキャン**、 **読み取り時にスキャン**、もしくは**実行時にスキャン**から選択します。なお、読み取り時にスキャンが行われた場合は、不明なプロセスによる感染があったかどうかを、新規ファイルもしくは新たなファイルバージョンの作成時にスキャンします。その他のケースでは、プログラムが読み取りを行う際にファイルをスキャンします。

- **ネットワークアクセスのスキャン**: ネットワークアクセスで不正プログラムをスキャンします。自身のコンピュータを、ネットワーク経由でウイルス対策がなされていない第三者のコンピュータと接続する場合に

は、この機能を有効にしてください。一方、スタンドアロン（ネットワークに未接続）環境、またはネットワーク内の全コンピュータにウイルス対策ソフトがインストールされている環境では、この機能は無効にしておいてください。これらの環境でこの設定を有効のままにしておくと、、重複スキャンが発生することがあり、コンピュータの動作速度の低下につながります。

- **ヒューリスティック**: ワクチンに情報がないウイルス特有の特徴をもつ新種ウイルスを検出します。この検出手法では、保護率を大幅に向上できますが、一方で、未感染ファイルを感染ファイルと判断することもあります。

- **アーカイブのスキャン**: アーカイブ（ZIP、RAR、またはPSTなどの拡張子を持つファイル）をスキャンします。アーカイブのスキャンには、多くの時間を要します。ウイルスガードが常時システムを監視している場合には、アーカイブを解凍する時にアーカイブ内のウイルスを検出するので、この機能は無効にして問題ありません。使用頻度が低い容量の大きなアーカイブのスキャンによるコンピュータの処理速度低下を防止するには、スキャンするアーカイブのサイズを制限します。

- **メールアーカイブのスキャン**: メールアーカイブをスキャンします。なお、本製品では、メールの送受信時にスキャンを実行しているので、通常はこの機能は無効にしていても問題はありません。メールアーカイブのスキャンは、アーカイブのサイズによっては数分間かかることがあります。

- **システム起動時にシステム領域をスキャン**: システム領域のスキャン実行タイミングをシステム起動時に設定します。この設定、もしくは**メディアの交換時にシステム領域をスキャン**のいずれかは常に有効にし、スキャン対象から除外しないでください。

- **メディアの交換時にシステム領域をスキャン**: システム領域のスキャン実行タイミングをメディア（CD/DVDなど）の交換時に設定します。この設定もしくは**システム起動時にシステム領域をスキャン**のいずれかは常に有効にし、スキャン対象から除外しないでください。

- **ダイヤラ/スパイウェア/アドウェア/リスクウェアのスキャン**: ダイヤラ 、スパイウェア、アドウェア、リスクウェアなどの不正プログラムをチェックします。これらの不正プログラムは、望ましくないインターネット接続を勝手に確立したり、ブラウザの閲覧履歴やキーボードへの入力（パスワードなど）を不正に盗みだし、情報漏洩や金銭的な被害に発展する恐れ

があります。

- **新しいファイルと変更したファイルのみスキャン**: この機能を有効にすると、以前実行したスキャンにおいて、安全と判断されているファイルで、かつしばらくの間、変更されていないファイルのスキャンをスキップします。スキャンの対象は、新規作成ファイルや変更されたファイルのみがスキャンされるようになり、スキャン速度を大幅に向上できます。

ウイルススキャン
オンデマンドスキャン用のスキャン設定を行います。

リアルタイム保護で利用できる項目です。

- **エンジンの種類**: ウイルススキャンに使用するエンジンを選択します。G Dataには、2 種類の高性能ウイルス検索エンジンを搭載し、世界最高レベルのウイルス検出率を実現しています。通常は、**2つのエンジン（最高検出力/推奨）**に設定してください。もしコンピュータの処理速度に問題がある場合は、1種類のエンジンのみを使用することにより、パフォーマンスを改善することもできます。

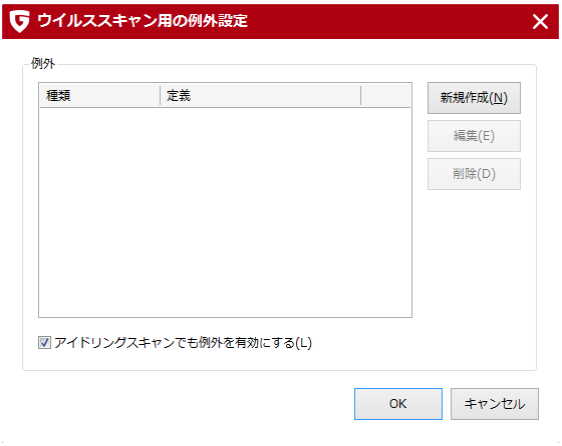
- **感染したファイル**: 感染ファイルが検出された場合の処理方法を設定します。デフォルト設定では、感染ファイルの処理方法をユーザーに確認します。なお、データを最高セキュリティで保護するには、**ウイルス駆除（不可能な場合は隔離）**に設定します。

- **感染したアーカイブ**: アーカイブファイル（RAR、ZIP または PST などの拡張子を持つファイル）を通常ファイルと別扱いするかどうかを設定します。なお、隔離されたアーカイブファイルは、元に戻す場合に破損する場合があります。感染したアーカイブは、**ユーザーの操作を待つ**を選択し、検出の度に処理方法をユーザーに選択させることをお勧めします。

- **高システム負荷時にはウイルススキャンを停止**: ユーザーがコンピュータ上で作業しない状態になると、スキャンが自動で実行されます。スキャン実行中にコンピュータを使用すると、スキャンは中断されます。中断されたスキャンは、再びコンピュータで作業をしない状態になった場合に再開されます。

例外

ウイルススキャンによるスキャンが不要なドライブ、ファイル、およびフォルダをスキャン対象から除外する設定を行います。



例外を設定するには、以下の手順に沿って行います。

1 **[例外]** を選択します。

2 **ウイルススキャン用の例外設定**のダイアログ画面で、**[新規作成]** を選択します。

3 次の**例外設定**の画面で、除外対象を**ドライブ**、**フォルダ**、**ファイル拡張子**を選択できます。

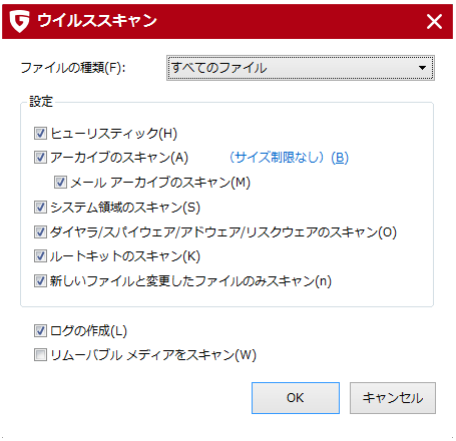
4 ドライブまたはフォルダを指定する場合は、対象を入力欄に直接入力するか、もしくは **[...]** をクリックして対象を指定します。拡張子を指定するには、拡張子を入力して **[OK]** を選択します。（例: 拡張子「**iso**」を持つファイルを例外設定するには、「**.iso**」もしくは「**iso**」と入力）

この手順を繰り返して例外設定行うことにより、自身の環境に適したウイルススキャンをカスタマイズできます。作成した例外設定は、**ウイルススキャン用の例外設定**画面の**例外**で表示され、編集や削除の操作は、それぞれ **[編集]** と **[削除]** から可能です。

アイドリングスキャンでも例外を有効にする: アイドリングスキャンは、ユーザーがコンピュータを利用しない時に自動的に起動するスキャン機能です。アイドリングスキャン中に、ユーザーが再び作業をはじめると、実行中のスキャンは中断されます。ユーザーはスキャンによるコンピュータ速度の低下に悩まされることはありません。ここではアイドリングスキャンでスキャン対象から除外するファイルやフォルダを指定します。

詳細設定

[詳細設定] からは、**ウイルススキャン**によるスキャンの詳細内容を確認したり、変更したりできます。



以下の項目を設定できます。

- **ファイルの種類**: ウイルススキャンの対象になるファイルの種類を指定します。**プログラムファイルとドキュメントのみ**を選択すると、速度優先でウイルススキャンします。
- **ヒューリスティック**: ウイルスデータベースに情報がないウイルス特有の特徴をもつ新種ウイルスを検出します。この検出手法では、保護率を大幅に向上できますが、一方で、未感染ファイルを感染ファイルと判断してしまう誤検出のケースもあります。
- **アーカイブのスキャン**: アーカイブ（ZIP、RAR、またはPSTなどの拡張子を持つファイル）をスキャンします。アーカイブのスキャンには、多くの時間を要します。ウイルスガードが常時システムを監視している場合には、アーカイブを解凍する時にアーカイブ内のウイルスを検出するので、この機能は無効にしておいてください。使用頻度が低い容量の大きなアーカイブのスキャンによるコンピュータの処理速度低下を防止するには、スキャンするアーカイブのサイズを制限します。
- **メールアーカイブのスキャン**: メールアーカイブをスキャンします。
- **システム領域のスキャン**: システム領域をスキャンします。この設定は

常に有効にしておいてください。

- **ダイヤラ/スパイウェア/アドウェア/リスクウェアのスキャン**: ダイヤラ 、スパイウェア、アドウェア、リスクウェアなどの不正プログラムをチェックします。これらの不正プログラムは、望ましくないインターネット接続を勝手に確立したり、ブラウザの閲覧履歴やキーボードへの入力（パスワードなど）を不正に盗みだし、情報漏洩や金銭的な被害に発展する恐れがあります。

- **ルートキットのスキャン**: 従来型のウイルス対策ソフトによる検出方法では検出が困難なルートキットをスキャンできます。

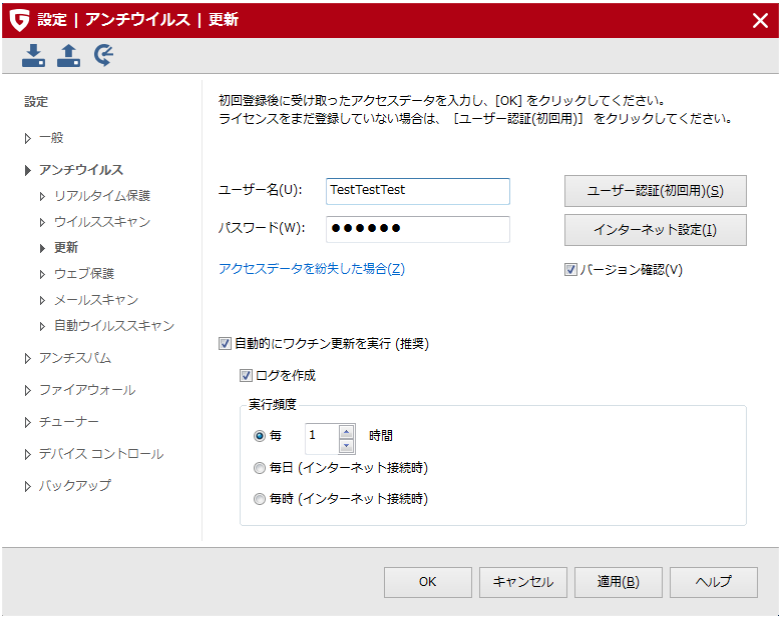
- **新しいファイルと変更したファイルのみスキャン**: この機能を有効にすると、以前スキャンしたことがあり、その際に安全と判断されたファイルのスキャンを省略します。スキャンの対象は、新規作成ファイルや変更されたファイルのみがスキャンされるようになり、スキャン速度を向上させることができます。

- **ログの作成**: ウイルススキャンのログを記録します。ログを閲覧するには、起動画面の右上のログアイコンをクリックします。

- **リムーバブルメディアをスキャン**: このチェックボックスを有効にすると、リムーバブルメディア（例: USBメモリ、USB外付けハードディスクなど）がコンピュータに接続された際に、ウイルススキャンを実行するかを確認するメッセージボックスが表示されます。

更新

ワクチンやプログラム更新が機能しない場合には、この領域で設定を確認してください。更新を利用するには、有効な**アクセスデータ（ユーザー名**と**パスワード）**が入力されている必要があります。アクセスデータは、製品の初回認証時に登録先メールアドレスに送信されています。



初めて認証を行う場合は、[ユーザー認証（初回用）] を選択します。 インターネット設定では、プロキシサーバーや更新ファイル用のサーバーを指定できます。

バージョンチェック

ワクチンファイルの差分更新を実行するかについて、設定できます。エンジンの破損や誤ってワクチンファイルを削除した場合以外は、通常、この設定は有効にしておいてください。

自動的にワクチン更新を実行

デフォルト設定の自動更新を利用しない場合にチェックを外します。なお、ワクチンが長期間更新されないと、コンピュータの保護レベルが著しく低下します。この設定は、特殊なケースを除き無効化しないでください。もし更新

間隔が短すぎる場合は、必要に応じて実行頻度を調節してください。
実行頻度内の、毎日（インターネット接続時）、もしくは毎時（インターネット接続時）という設定は、コンピュータがインターネット接続中かどうかを判断し、インターネットに接続している場合のみ更新処理を行う設定です。これはコンピュータを外へ持ち出している場合などに適した設定で、不必要な処理を減らす事ができます。

ログを作成: ワクチン更新やウイルス検出などをログとして記録します。起動画面の右上にあるログアイコンをクリックすると、ログを閲覧できます。

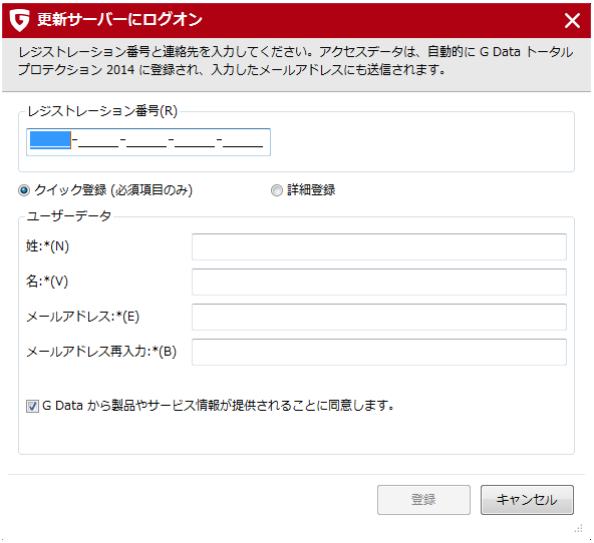
ユーザー認証（初回用）
ユーザー認証が完了していない場合は、ここから**レジストレーション番号**を入力して認証を行うことができます。ボックス製品を購入された場合は、レジストレーション番号はユーザー登録用紙に記載されています。ダウンロード版を購入された場合は、メールで送信されています。

製品を認証するには、**[ユーザー認証（初回用）]** をクリックすると現れる画面に、**レジストレーション番号**、**姓**、**名**、**メールアドレス（PC用）**を入力し、**[登録]** をクリックします。認証が正常に行われると、**「登録に成功しました。アクセスデータは自動的に本製品に登録され、メールでもアクセスデータが送信されます。」**というメッセージが表示されます。**[OK]** をクリックして、この画面を閉じます。

> 注意: アクセスデータは、ここで登録したメールアドレスに送信されます。メールアドレス入力の際は、誤入力のないようにご注意ください。アクセスデータは、再インストールまたは2台目以降のPCを認証する際（複数台版を購入の場合）に必要です。

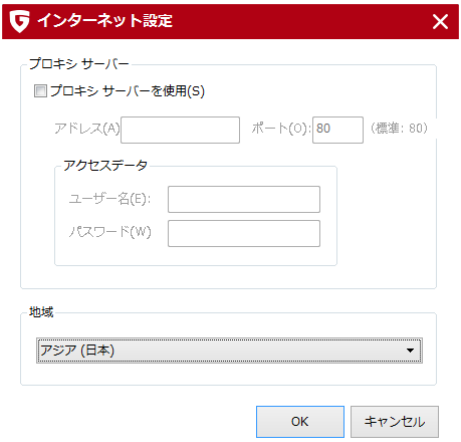
認証後は、ユーザー名とパスワードの入力欄に生成されたアクセスデータが自動的に入力されます。これで更新を実行できるようになります。

> **認証に失敗する場合**
> まず、ブラウザを使ってインターネットに正常に接続されているか確認してください。ブラウザでインターネット閲覧できるにもかかわらず更新できない場合は、プロキシサーバーに問題がある可能性があります。この場合は、**インターネット設定** を選択して、プロキシサーバーに入力されている情報を確認してください。



インターネット設定

プロキシサーバー を使用する環境では、**プロキシサーバーを使用**にチェックを入れてください。この設定は、インターネット更新が正常に機能しない場合にのみ変更します。プロキシサーバーの入力欄で入力する情報については、システム管理者またはインターネット接続プロバイダに確認してください。アクセスデータは必要に応じて入力してください。



プロキシサーバー: プロキシサーバーは、ネットワーク内のPCからのリクエストを束ねてインターネットに接続します。社内ネットワークなどにプロキシサーバーが導入されている場合は、**プロキシサーバーを使用**にチェックを入れ、必要な情報を入力することで、更新が利用にできるようになります。

ウェブ保護
ウェブ保護を有効にすると、ウェブ閲覧中もコンピュータをマルウェアから保護することができます。ウェブ保護では次の設定が可能です。

- **インターネットコンテンツ（HTTP）のスキャン**: インターネット閲覧するだけで感染する危険がある、ウェブページ経由のウイルスをスキャンします。ユーザーが閲覧しようとしたコンテンツで不正プログラムを検出すると、そのコンテンツの実行をストップして、コンピュータを感染から守ります。なお、ウイルスが検出された場合、ウェブページは表示されません。この設定を有効にするには、**インターネットコンテンツ（HTTP）のスキャン**にチェックを入れます。

  ウェブコンテンツのスキャンを無効にした場合は、**ウイルスガード**は必ず有効にしてください。不正プログラムの実行時に、ウイルスガードがこれを検出します。

  特定サイトを例外に設定するには、例外の項を参照してください。[詳細設定] からは、インターネットコンテンツ関連の設定を行うことができます。

- **フィッシング保護:** オンラインバンキング、オンラインショップ、ネットオークションの偽サイトに誘導し、顧客データやログイン情報を盗むフィッシング詐欺サイトをブロックします。インターネットを閲覧する時は、常時有効化することをお勧めします。

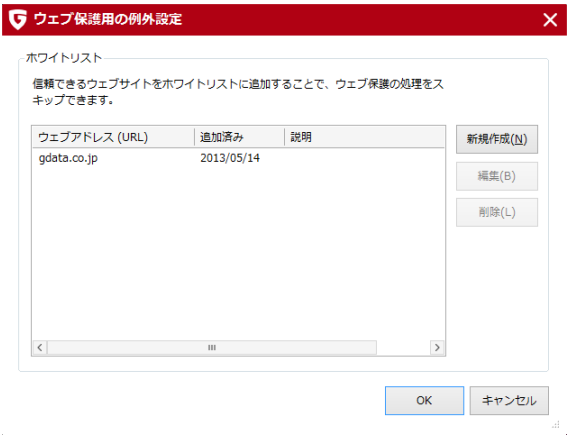
- **感染したウェブページのアドレスを送信**: 危険と判断されたウェブページの情報を G Data へ自動送信します。なお、このアドレスの送信は、匿名で処理されます。送信元が特定できるデータは送信されません。収集データは、ユーザーがインターネットをより安全に利用できるために役立てられます。

- **バンクガードによる保護**: ネットバンキングを標的とするバンキング系トロイの木馬による攻撃（man-in-the-middle攻撃）を検出し、リアルタイムで保護します。バンキング系トロイの木馬は、金銭的被害をもた

らす悪質な不正プログラムで、現在、世界各国で猛威を振るっています。銀行サイトがオンライン取引の暗号化をしていても、攻撃は復号化されたブラウザ上で行われるため、通常のウイルス対策ソフトでは攻撃の回避が困難でした。G Data では、ネットワークライブラリをリアルタイムでチェックすることにより、man-in-the-middle攻撃によるブラウザの不正操作を保護します。

例外
ウェブサイトを例外として設定するには、次の手順に沿って行います。

1 **[例外]** をクリックします。そうすると、**ウェブ保護用の例外設定**の画面が開きます。 この画面では、ユーザーが安全なサイトとして登録したページが表示されます。



2 例外のウェブサイトを **ウェブ保護用例外**に追加するには、**[新規作成]** をクリックします。入力画面が開くので、URL の欄にウェブページのアドレス（例： www.gdata.co.jp）と、必要に応じて**説明**の欄に登録の理由などを入力します。

3 **[OK]** をクリックすると、ウェブページが例外サイトとして追加され、ウェブ保護の対象から除外されます。

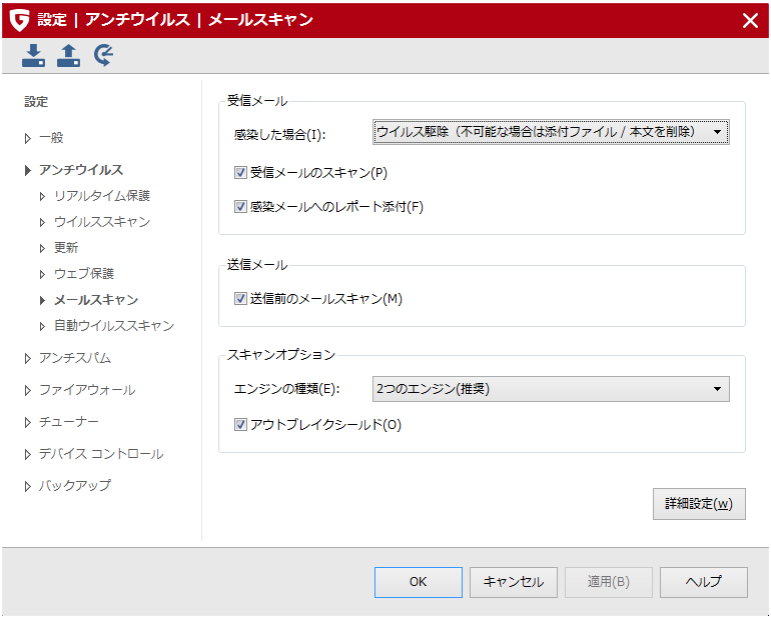
例外に登録したウェブページの編集や編集は、登録した項目を選択し、編集の場合は **[編集]** を、削除の場合は **[削除]** をクリックします。

詳細設定
ウェブ保護が監視するサーバーポート番号を設定します。デフォルト設定では、通常のインターネット閲覧に使用する 80 が設定されています。

- **ブラウザのタイムアウトを防止**: **インターネットコンテンツ（HTTP）のスキャン**にチェックを入れた場合、ウェブコンテンツをブラウザに表示する前に不正ルーチンのチェックが行われます。この処理はデータ量によっては処理時間がかかり、ブラウザが表示データをすぐに受信できないため、エラーメッセージが表示されることがあります。**ブラウザのタイムアウトを防止**にチェックを入れると、このエラーメッセージが表示されず、コンテンツ全体のチェックが終了するとウェブページが通常どおり表示されるようになります。

- **ダウンロードの容量制限**: 指定したサイズを超過したダウンロードファイルでの**インターネットコンテンツ（HTTP）のスキャン**を解除します。この容量制限を利用することで、**インターネットコンテンツ（HTTP）のスキャン**によるインターネットの通信速度低下を回避できるます。なお、容量制限した場合は、ウイルスガードは必ず有効にしておいてください。

メールスキャン
メールスキャンは、送受信メールや添付ファイルでウイルススキャンする機能です。メールスキャンで検出した添付ファイルは、削除や修復の操作ができます。



注意: **Microsoft Outlook** には、専用プラグインがインストールされます。このプラグインは、Outlook 上でより簡単なウイルスチェックを実現するツールです。メールスキャンで設定できる POP3/IMAP ベースの保護と全く同じ機能を提供します。メールまたはフォルダのスキャンを実行するには、Outlook メニューバーの **[ツール] > [フォルダのウイルスをスキャン]** を選択します。

受信メール
受信メールでは、次の設定が可能です。

- **感染した場合**: 感染メールが検出された場合の処理方法を設定します。コンピュータ環境に応じて、最適な設定を選択してください。通常は、**ウイルス駆除（不可能な場合は添付ファイル / メール本文を削除）**の使用をお勧めします。

- **受信メールのスキャン**: インターネット接続中の全受信メール に対して、ウイルススキャンを実行します。

- **感染メールへのレポート添付**: ウイルスが検出された場合、感染メールの件名欄に**「ウイルス」**という警告を挿入します。また、メール本文の先頭に**「注意！このメールはウイルスに感染しています」**というメッセージ、ウイルスの名称、ウイルスの駆除または感染ファイルを修復したなどの情報を表示します。

送信メール
送信メールでは、次の設定が可能です。

- **送信前のメールスキャン**: ウイルス添付メールの外部送信を防ぐために、送信前にチェックします。この機能が有効な場合に、ウイルス添付メールを送信しようとすると、**「メール [件名] には次のウイルスがあります: [ウイルス名]」**というメッセージが表示され、メールの送信はブロックされます。

スキャンオプション
スキャンオプションでは、基本的なウイルススキャンの基本的な設定を行います。次の設定が可能です。

- **エンジンの種類**: ウイルススキャンに使用するエンジンを選択します。G Dataには、2 種類の高性能ウイルス検索エンジンを搭載し、世界最高レベルのウイルス検出率を実現しています。通常は、**2つのエンジン（最高検出力/推奨）**に設定してください。もしコンピュータの処理速度に問題がある場合は、1種類のエンジンのみを使用することにより、パフォーマンスを改善することもできます。

- **アウトブレイクシールド**: パンデミック型のウイルス感染メールを常時監視してブロックするクラウド型機能、アウトブレイクシールド（OutbreakShield）を有効/無効を設定します。アウトブレイクシールドを有効にすると、受信メールにチェックサムが作成され、クラウド上のアンチスパムブラックリストと照会が行われます。これにより、ワクチンに依存することなく、ウイルスが最初に発見された時点から数十秒から数分内でウイルスメールとして検出できます。

詳細設定
メールプログラムに**標準ポート**を割り当てていない場合には、メールの送受信に使用する**ポート**を**サーバーポート番号**の欄に入力してください。**[標準]** をクリックすると、自動的に標準のポート番号にリセットされます。複数のポートをスキャンさせたい場合は、コンマ（ , ）でそれぞれのポート番号を区切って入力してください。

> **注意**: **Microsoft Outlook** には、専用プラグインがインストールされます。このプラグインは、Outlook 上でより簡単なウイルスチェックを実現するツールです。Outlook プラグインを使うと、**Outlook** 上で簡単な操作でメールスキャンができるようになります。スキャンを実行するには、スキャンする対象のメールまたはフォルダを選択し、G Data アイコンをクリックして実行する操作を選択します。

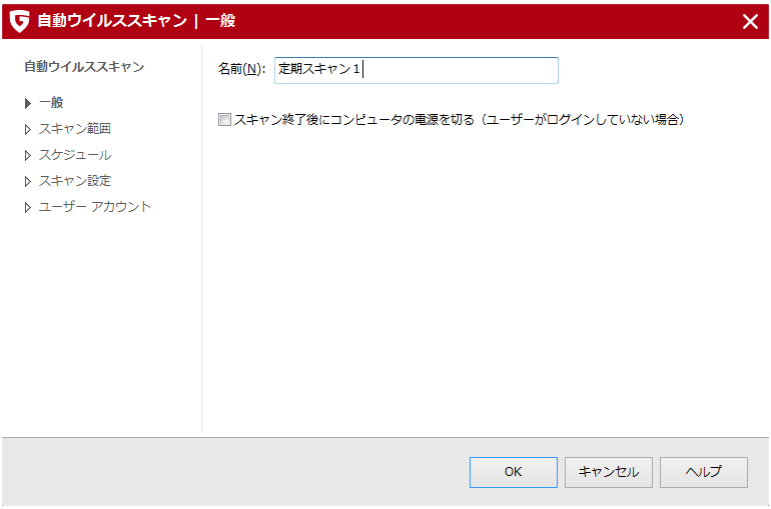
G Data のメールスキャンは、メールプログラムが実際にメールを受信する以前に処理を行うため、大量のメールを受信する場合やインターネット回線速度が遅い環境では、メールプログラムがタイムアウトのエラーメッセージを表示することがあります。この原因は、メールスキャンによるスキャンで、メールプログラム側でのメール受信で遅延が発生するためです。**メールクライアントのタイムアウトを防止**にチェックを入れると、タイムアウトエラーが表示されなくなります。受信メールは、スキャン完了次第、メールプログラムに引き渡されます。

自動ウイルススキャン
ユーザーがコンピュータを使用していない時にスキャンが自動実行されるアイドリングスキャン機能やスキャン対象、スキャン実行日時や頻度、エンジンの種類などをカスタムしたスケジュールスキャンを設定できます。

ウイルススキャンのスケジュール設定で、**[新規作成]** をクリックします。ダイアログ画面が開くのでまず名前を入力し、必要な項目を設定してください。例えば、ダウンロードしたファイルを毎日特定の時間にスキャンする場合は、**スキャン範囲**の**次のフォルダとファイルをスキャン**を選択し、**[選択]** ボタンから対象フォルダを選択します。次に**スケジュール**の**実行頻度**で**毎日**を選択、そして時間を設定して、[OK] をクリックすれば設定は完了です。

設定 | アンチウイルス | 自動ウイルススキャン
設定
一般
アンチウイルス
リアルタイム保護
ウイルススキャン
更新
ウェブ保護
メールスキャン
自動ウイルススキャン
アンチスパム
ファイアウォール
チューナー
デバイス コントロール
バックアップ
アイドリングスキャン
システムがアイドリング状態になった場合に、自動的にスキャンを行います。
有効(推奨)(S)
ウイルススキャンのスケジュール設定(G)
名前
実行
次回の起動
前回の起動
今すぐ開始(J)
新規作成(N)
プロパティ(E)
削除(L)
OK
キャンセル
適用(B)
ヘルプ

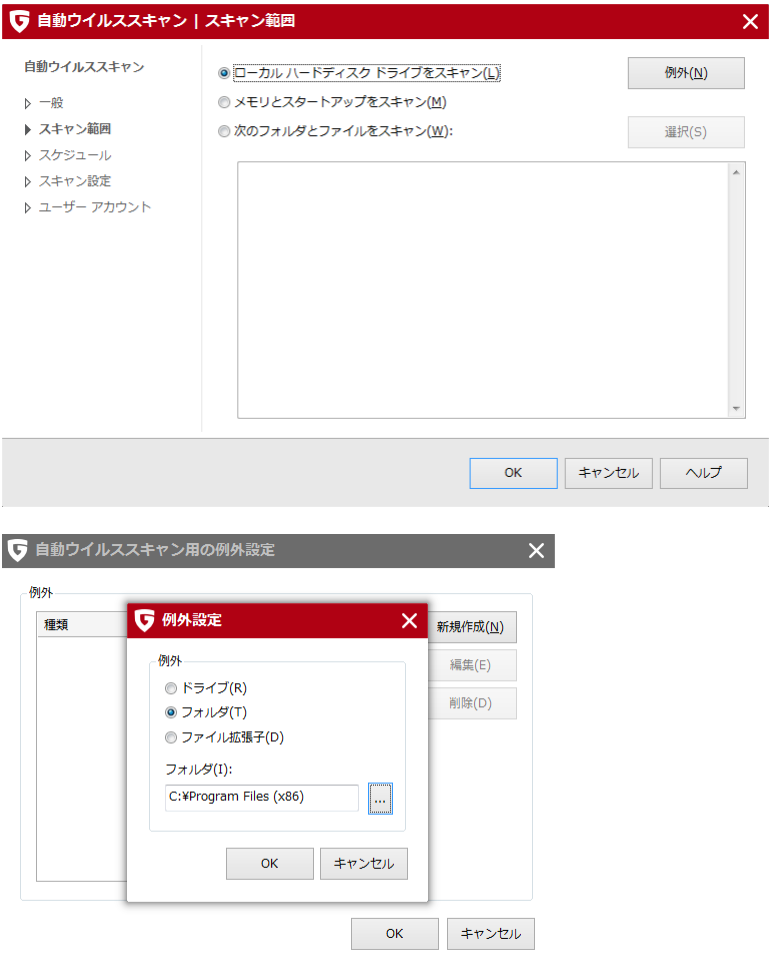
一般
新規作成する自動ウイルススキャンジョブに名前をつけます。ジョブにはわかりやすい名前をつけてください。



スキャン終了後にコンピュータの電源を切る（ユーザーがログインしていない場合）にチェックを入れると、スキャン後にコンピュータを自動的にシャットダウンします。

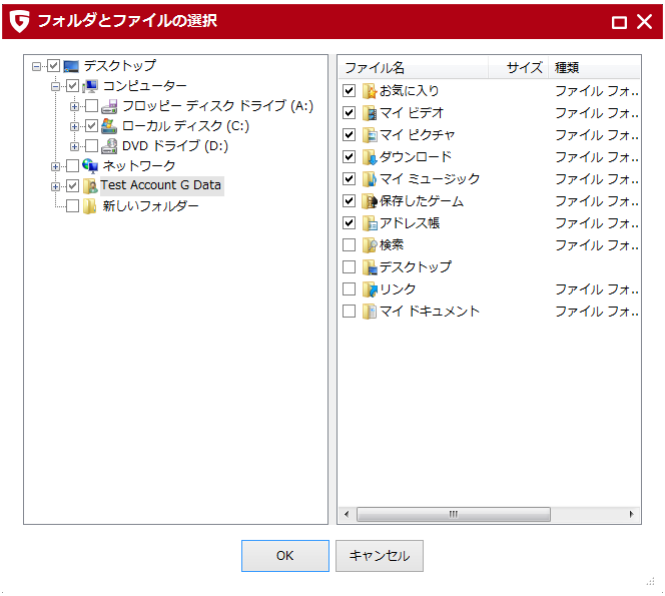
ジョブ: 実行されるウイルススキャン処理の単位を**ジョブ**と呼びます。

スキャン範囲
ウイルススキャンを実行する対象を設定します。スキャンの対象は、**ローカルのハードディスクドライブ**、**メモリとスタートアップ**、**次のフォルダとファイルをスキャン**から選択できます。次のフォルダとファイルをスキャンを選択した場合は、**[選択]** をクリックすると対象を指定します。



フォルダとファイルの選択: フォルダのツリー構造で「+」をクリックするとそのフォルダが展開し、フォルダの内容がファイルビューに表示されます。チェックが入っているフォルダまたはファイルがスキャンの対象になります。

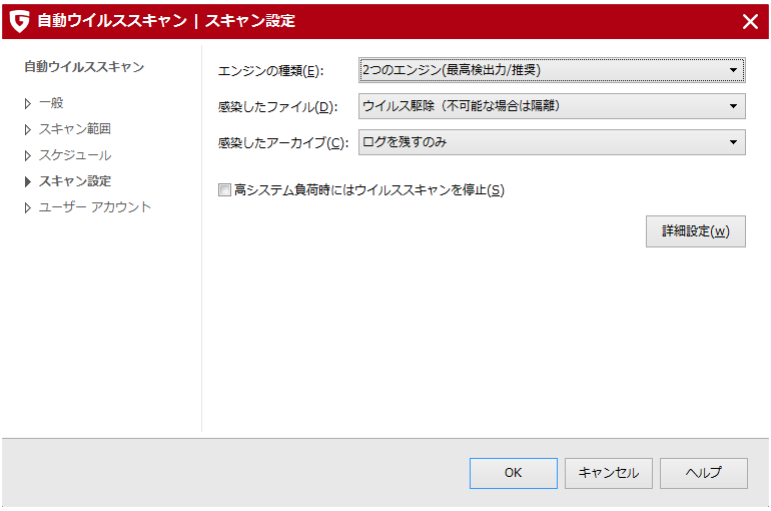
なお、フォルダ内ですべてのファイルがマークされるとチェックマークは黒で表示されます。一部のファイルが選択されていないフォルダは、グレーのチェックマークで表示されます。



スケジュール
ジョブを実行するタイミングを設定します。実行のタイミングは、**実行頻度**と**時間**を組み合わせて設定します。**実行頻度**で**システム起動時**を選択した場合は、**時間**は非表示となります。

- **スケジュール実行後にコンピュータの電源が切れていた場合、次回の起動時にジョブを実行**: コンピュータを起動していなかったため実行できなかったスキャンジョブを、コンピュータの次回起動した時に自動的に実行します。
- **バッテリモードでは実行しない**: ノートパソコン用の設定です。バッテリー駆動時はスキャンジョブを実行せずに、AC電源での駆動時にスキャンジョブを実行します。

スキャン設定
自動ウイルススキャン用のスキャン設定について定義します。



- **エンジンの種類**: ウイルススキャンに使用するエンジンを選択します。G Dataには、2 種類の高性能ウイルス検索エンジンを搭載し、世界最高レベルのウイルス検出率を実現しています。通常は、**2つのエンジン（最**

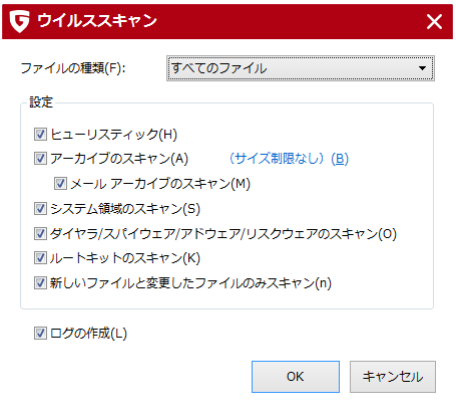
高検出力/推奨）に設定してください。もしコンピュータの処理速度に問題がある場合は、1種類のエンジンのみを使用することにより、パフォーマンスを改善することもできます。

- **感染したファイル**: 感染ファイルが検出された場合の処理方法を設定します。デフォルト設定では、ウイルスが検出されるとウイルスと感染ファイルについてのログが残されます。最高セキュリティで保護するには、**ウイルス駆除（不可能な場合は隔離）**に設定します。

- **感染したアーカイブ**: アーカイブファイル（RAR、ZIP または PST などの拡張子を持つファイル）を通常ファイルと別扱いするかどうかを設定します。なお、アーカイブファイルを隔離すると、元に戻す場合にファイルが破損する場合があります。感染したアーカイブは、**ログを残すのみ**を選択し、検出の度に処理方法をユーザーが選択することをお勧めします。

- **高システム負荷時にはウイルススキャンを停止**: ユーザーがコンピュータ上で作業しない状態になると、スキャンが自動で実行されます。スキャン実行中にコンピュータを使用すると、スキャンは中断されます。中断されたスキャンは、再びコンピュータで作業をしない状態になった場合に再開されます。

[詳細設定] からはスキャン詳細設定の編集や確認ができます。



次の設定が可能です。

- **ファイルの種類**: スキャン対象とするファイルの種類を選択します。

- **ヒューリスティック**: ウイルスデータベースに情報がないウイルス特有の特徴をもつ新種ウイルスを検出します。この検出手法では、保護率を大幅に向上できますが、一方で、未感染ファイルを感染ファイルと判断してしまう誤検出のケースもあります。

- **アーカイブのスキャン**: アーカイブ（ZIP、RAR、またはPSTなどの拡張子を持つファイル）をスキャンします。アーカイブのスキャンには、多くの時間を要します。ウイルスガードが常時システムを監視している場合には、アーカイブを解凍する時にアーカイブ内のウイルスを検出するので、この機能は無効にしておいてください。使用頻度が低い容量の大きなアーカイブのスキャンによるコンピュータの処理速度低下を防止するには、スキャンするアーカイブのサイズを制限します。

- **メールアーカイブのスキャン**: メールアーカイブをスキャンします。

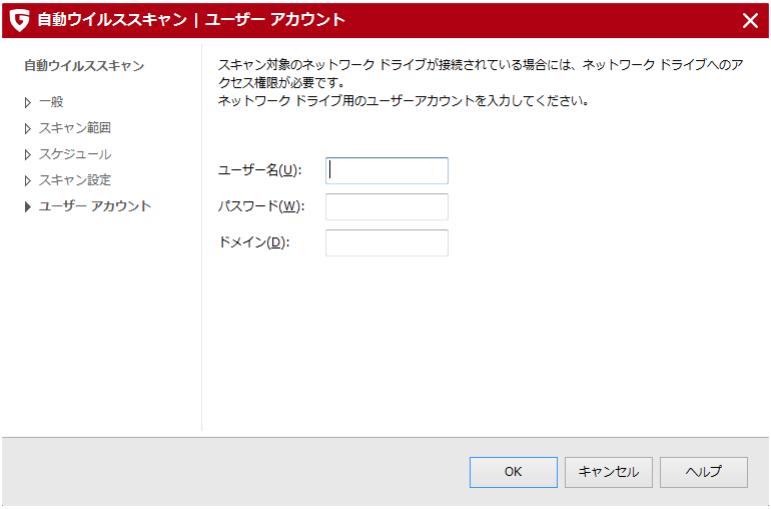
- **システム領域のスキャン**: システム領域をスキャンします。この設定は常に有効にしておいてください。

- **ダイヤラ/スパイウェア/アドウェア/リスクウェアのスキャン**: ダイヤラ 、スパイウェア、アドウェア、リスクウェアなどの不正プログラムをチェックします。これらの不正プログラムは、望ましくないインターネット接続を勝手に確立したり、ブラウザの閲覧履歴やキーボードへの入力（パスワードなど）を不正に盗みだし、情報漏洩や金銭的な被害に発展する恐れがあります。

- **ルートキットのスキャン**: 従来型のウイルス対策ソフトによる検出方法では検出が困難なルートキットをスキャンできます。

- **ログの作成**: ウイルススキャンのログを記録します。ログを閲覧するには、起動画面の右上のログアイコンをクリックします。

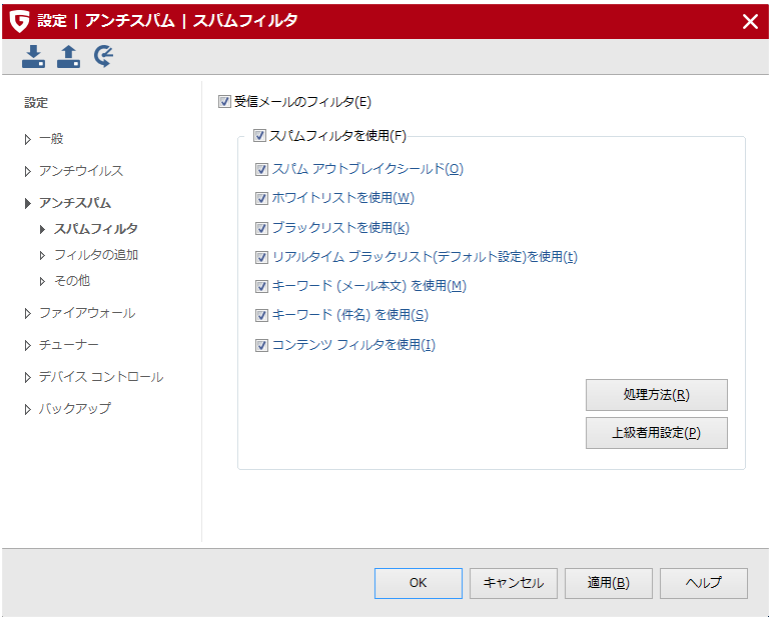
ユーザーアカウント
コンピュータがネットワークに接続されている環境で、接続先もスキャン対象とする場合は、接続先へのアクセス権が必要となります。アクセスに必要な**ユーザー名**、**パスワード**、**ドメイン**を入力してください。



アンチスパム

スパムフィルタ

スパムフィルタは、スパムメールが持つ特長をもとに数値を算出し、スパムメールを効果的にブロックする機能です。スパムフィルタを有効にするには、**スパムフィルタを使用**にチェックを入れます。



スパムフィルタの項目の有効/無効の切換えはチェックボックスで行います。各スパムフィルタ項目の設定を変更するには、項目をクリックすると表示される画面から行います。スパムフィルタには、次の項目があります。

- **スパム アウトブレイクシールド**: パンデミック型のウイルス感染メールを常時監視してブロックするクラウド型機能、アウトブレイクシールド（OutbreakShield）を有効/無効を設定します。アウトブレイクシールドを有効にすると、受信メールにチェックサムが作成され、クラウド上のアンチスパムブラックリストと照会が行われます。これにより、ワクチンに依存することなく、ウイルスが最初に発見された時点から数十秒から数分内でウイルスメールとして検出できます。プロキシサーバーを使用している環境では、**[インターネット設定]** をクリックし、設定の変更を行ってください。この設定はアウトブレイクシールドが機能しない場合にのみ変更してください。

- **ホワイトリストを使用**: 特定のメールアドレスやドメインから送信されるメールを、スパムとして判定しないように設定できます。ホワイトリストに登録するには、**ホワイトリストを使用**を選択すると表示されるウィンドウ上の **[新規作成]** をクリックし、**送信者アドレス/ドメイン**の欄にスパム判定から除外するメールアドレス（例：newsletter@gdata.co.jp）またはドメイン（例：gdata.co.jp） を入力して、**[OK]** をクリックします。そうすると、入力された送信者またはドメインからのメールを、スパムではないと判定されるようになります。

  また、**[インポート]** をクリックすると、既存のメールアドレスまたはドメインのリストをホワイトリストに追加できます。インポート用のリストを作成するには、Windows の「メモ帳」などのテキストエディタプログラムを利用し、テキスト形式（txt ファイル）で作成します。また、キーワードリストは、必ず1 件 1 行ずつ、上から順に入力してください。**[エクスポート]** からは、ホワイトリストをテキスト形式で書き出します。

- **ブラックリストを使用**: 特定のメールアドレスやドメインから送信されるメールを、スパムとして判定するように設定できます。ブラックリストに登録するには、**ブラックリストを使用**を選択すると表示されるウィンドウ上の **[新規作成]** をクリックし、**送信者アドレス/ドメイン**の欄にスパム判定するメールアドレス（例：newsletter@spam.co.jp）またはドメイン（例：spam.co.jp）を入力して、**[OK]** をクリックします。そうすると、入力された送信者またはドメインからのメールは、自動的にスパムと判定されるようになります。

  また、**[インポート]** をクリックすると、既存のメールアドレスまたはドメインのリストをブラックリストに追加できます。インポート用のリストを作成するには、Windows の「メモ帳」などのテキストエディタプログラムを利用し、テキスト形式（txt ファイル）で作成します。また、キーワードリストは、必ず1 件 1 行ずつ、上から順に入力してください。**[エクスポート]** からは、上述のブラックリストをテキスト形式で書き出します。

- **リアルタイムブラックリストを使用**: スパム送信に使用されているサーバーのブラックリストをもとに、受信メールがスパムメールであるかどうかを確かめます。サーバーがリストに掲載されていれば、スパムの可能性は高くなります。この設定はデフォルト設定のままでの使用をお勧めますが、カスタムも可能です。

- **キーワード（メール本文）を使用**: **メール本文**に使用されている単語をもとに、スパムメールかどうかを判断します。リスト内の 1 個以上の単

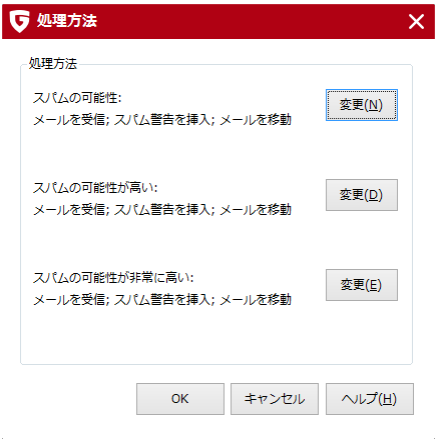
語がメール本文に使用されていると、スパムの可能性が高まります。**キーワード**のリストは、**[新規作成]**、**[編集]**、**[削除]**が可能です。また、**[インポート]** をクリックすると、自身で作成した**キーワード**リストを追加できます。インポート用のリストを作成するには、Windows の「メモ帳」などのテキストエディタプログラムを利用し、テキスト形式（txt ファイル）で作成します。また、キーワードリストは、必ず1 件 1 行ずつ、上から順に入力してください。**[エクスポート]** からは、既存のキーワードリストをテキスト形式で書き出します。 **完全なキーワードのみ検索**にチェックを入れると、完全に一致する単語だけを検索します。

- **キーワード（件名）を使用**: **メールの件名**に使用されている単語をもとに、スパムメールかどうかを判断します。リストの 1 語以上が件名に使用されていると、スパムの可能性が高まります。キーワードの編集は、**キーワード（メール本文を使用）**と同様の操作で行います。

- **コンテンツフィルタを使用**: **コンテンツフィルタ**は自己学習型フィルタで、**メール本文**の単語を基準にしてスパムの可能性を計算します。このフィルタは、変更できない単語リストだけを基準にして機能するのではなく、新着メールが届くたびに学習してリストを拡張していきます。**[テーブルコンテンツを検索]** をクリックすると、メールをスパムに分類するコンテンツフィルタが使用している単語リストを表示できます。**[テーブルをリセット]** をクリックすると学習したテーブルの内容がすべて削除され、自己学習型コンテンツフィルタが学習プロセスを最初からやり直します。

処理方法

スパムフィルタによるスパムメールへの応答方法を定義します。スパムの疑いがあるメールの処理方法は、スパム判定された3種類の段階で設定できます。



- **スパムの可能性があるメール:** スパムの特徴を持つメールが検出された場合の処理ルールを設定します。ここに振り分けられたメールには、受信者が配信を希望するニュースレターが紛れ込むこともあります。そのため、受信者にはスパムの可能性を通知する設定をお勧めします。

- **スパムの可能性が高いメール:** スパムの要素を多数持っているメールが検出された場合の処理ルールを設定します。この中にはまれに受信者が配信を希望するメールが含まれることもあります。

- **スパムの可能性が非常に高いメール:** スパムメールの要件をすべて満たすメールが検出された場合の処理ルールを設定します。ここに配信を希望するメールが紛れ込むことはほとんどありません。ここに振り分けられたメールは受信拒否することをお勧めします。

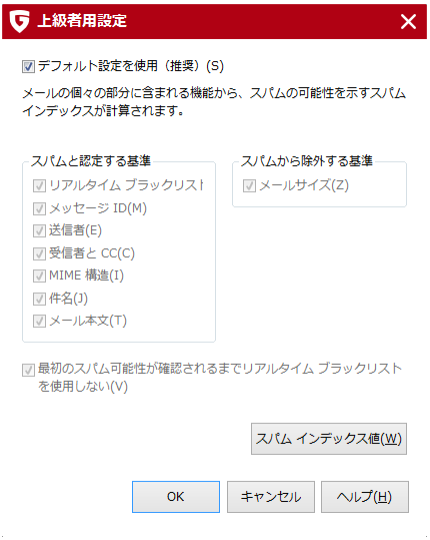
この3 種類の処理方法は、それぞれ独自にカスタマイズできます。変更を行うには、**[変更]** をクリックします。

[変更] を押すと表示される画面内にある**メールを拒否**にチェックを入れると、スパムと判断されたメールを受信トレイに入れません。また、**メールの件名**と**本文にスパム警告を挿入**にチェックを入れると、スパムと判断されたメールに警告を挿入します。Microsoft Outlook を利用している場合は、**メールをフォルダに移動**からスパムの疑いのあるメールを受信フォルダ内の任意のフォルダ（デフォルト設定：アンチスパム）に移動できます。

> **メモ**: Microsoft Outlook を使用していない場合でも、スパムと判断されたメールをフォルダに移動できます。メールを移動するには、件名欄に警告 ([Spam] など) を挿入し、使用しているメールプログラムで、警告されたメールを別のフォルダに移動させるルールを作成します。

上級者用設定

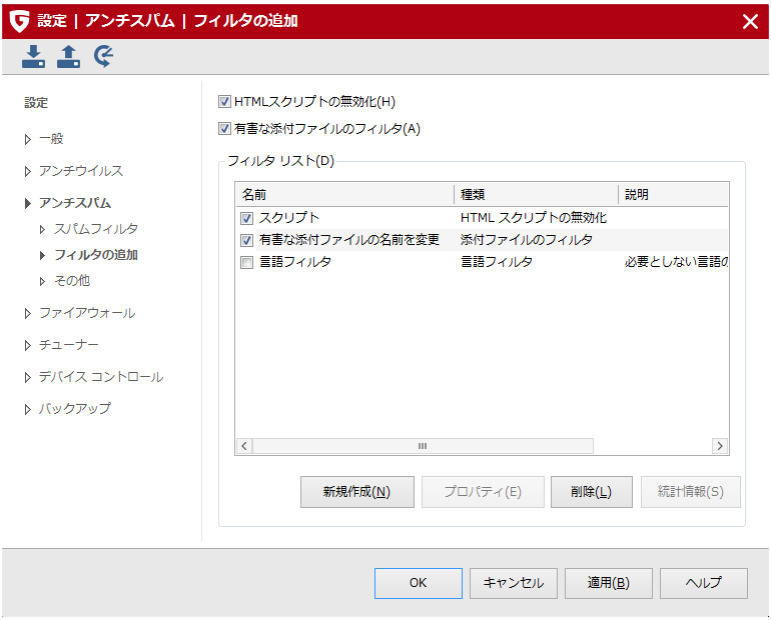
スパム検出の基準として使用されるスパムインデックス値を詳細にカスタマイズできる上級者用の設定です。専門知識を必要とする設定のため、通常はデフォルト設定のままで使用する事をお勧めします。



フィルタの追加
デフォルト設定では次のフィルタが有効になっていますが、チェックを外すことで無効にできます。

- **HTMLスクリプトの無効化:** このフィルタは、メールのHTML部分のスクリプトを無効にします。HTMLスクリプトは、ウェブページで利用されるスクリプトですが、コンピュータを感染させるために メールに埋め込まれて悪用されることがあります。

- **有害な添付ファイルのフィルタ:** メールに添付されている危険な添付ファイルをフィルタします。多くのメールウイルスは、EXEファイルや画像（動画または音楽）ファイルに仕掛けられたVBスクリプトや隠し実行ファイルが含まれる添付ファイルを通して広がります。メールの添付ファイルを実行する際は、十分に注意してください。場合によっては、送信者に確認するのも感染から有効な手段の１つです。



新規フィルタを追加するには、**[新規]** をクリックし、表示されたダイアログ

画面で**フィルタの種類**を選択して**[OK]** をクリックしてください。続いて選択した**フィルタ**の設定アシスタント画面が開くので、必要な情報を入力して **[OK]** をクリックします。フィルタを削除するには、対象のフィルタを選択して、**[削除]** をクリックします。

以下が選択可能なフィルタの種類です。各フィルタの設定方法を解説します。

- **添付ファイルのフィルタ**: メールに添付されている危険な添付ファイルをフィルタします。

  ファイル拡張子では、フィルタに適応する拡張子を指定します。指定できる拡張子の種類は、実行ファイル（EXEファイルやCOMファイルなど）の他、画像／動画／音楽ファイル（MPEG／AVI／MP3／JPEGなど）や圧縮ファイル（ZIP／RAR／CABなど）の拡張子もフィルタできます。複数の拡張子を指定する際は、それぞれの拡張子をコンマ（,）で区切ります。

  添付ファイルのみ名前を変更にチェックを入れると、フィルタする添付ファイルは自動削除されずに、ファイル名が変更されます。ファイル名を変更すると、実行ファイルや実行可能なスクリプトやマクロを含むMicrosoft Office 形式のファイルをクリックしただけでは実行できないので、誤ってクリックしての感染などを未然に防ぐことができます。ファイル名が変更されたファイルを実行するには、ユーザーはファイルを任意の場所に保存し、本製品によって付与された拡張子（デフォルト設定では_danger）を消去する必要があります。危険とみなされたファイルに付与する拡張子はユーザーが自由に設定できます。**添付ファイルのみ名前を変更**にチェックを入れない場合は、フィルタされたファイルはすぐに削除されます。

  メール本文にメッセージを挿入にチェックを入れると、危険な添付ファイルが含まれていた場合、判断されたメールにテキストを挿入し、添付ファイルが削除された（もしくは名前が変更された）ことをユーザーに知らせます。

- **コンテンツフィルタ**: コンテンツフィルタは、特定のテーマまたはテキストを含むメールの受信をブロックします。コンテンツフィルタを設定するには、まず**検索基準**に、フィルタするキーワードと表現を入力します。論理演算子 AND および OR を使うと、キーワードや表現を複数入力できます。

  検索範囲では、メールのどの部分でこの表現を検索するかを指定します。**ヘッダ**では、送信者および受信者のメールアドレス、件名、メールプログラムの情報、プロトコル、送信者情報がフィルタの対象となりま

す。**件名**では、件名欄の内容だけをチェックします。

メール本文では純粋なテキストメール 、**HTML テキスト**ではHTMLメールをチェックします。**埋め込みメール**では、コンテンツフィルタの対象を受信メールの本文に添付ファイルが埋め込まれているメールをフィルタ対象とするかどうかを指定します。

処理方法では、スパムと判断されたメールの処理方法を設定します。**メールの件名と本文に警告を挿入**にチェックを入れると、疑わしいメールの件名欄の件名の前に**「スパム」**または**「注意」**などの警告**（[件名に追加する文字]）**を挿入できます。

メールを拒否を有効にすると、メールプログラムはこの警告が件名欄に挿入されたメールを受信しません。スパムの疑いがある場合には、件名欄ではなく実際のメール本文の前にテキストを挿入することもできます**（[本文中のメッセージ]）**。

Microsoft Outlook （※Outlook Express や Windows Mail では不可）を使用している場合 、スパムの疑いのあるメールを受信トレイ内の任意のフォルダに移動できます **（[メールをフォルダに移動]）**。移動先のフォルダは、**フォルダ名**に入力すると新規作成できます。

- **送信者フィルタ**: 送信者フィルタは、特定の送信者から送られてきたメールの受信をブロックします。送信者フィルタを設定するには、**送信者 / ドメイン**に、ブロックする送信者のメールアドレス とドメイン名を入力します。複数の送信者を登録する場合には、メールアドレスをセミコロン (;) で区切ります。

  処理方法では、スパムと判断されたメールの処理方法を設定します。**メールの件名と本文に警告を挿入**にチェックを入れると、疑わしいメールの件名欄の件名の前に「スパム」または「注意」などの警告（件名に追加する文字）を挿入できます。

  メールを拒否 を有効にすると、メールプログラムはこの警告が件名欄に挿入されたメールを受信しません。スパムの疑いがある場合に、件名欄ではなく実際のメール本文の前にテキストを挿入することもできます**（本文中のメッセージ）**。

  Microsoft Outlook を使用している場合（※Outlook Express または Windows Mail では不可）、スパム疑惑のあるメールを受信トレイ内の自由に定義できるフォルダに移動することができます**（メールをフォルダに移動）**。本製品は、**フォルダ名**の欄にフォルダを定義すれば直接フォルダを作成する機能を備えています。

- **言語フィルタ**: 言語フィルタでは、特定の言語で書かれたメールをスパム

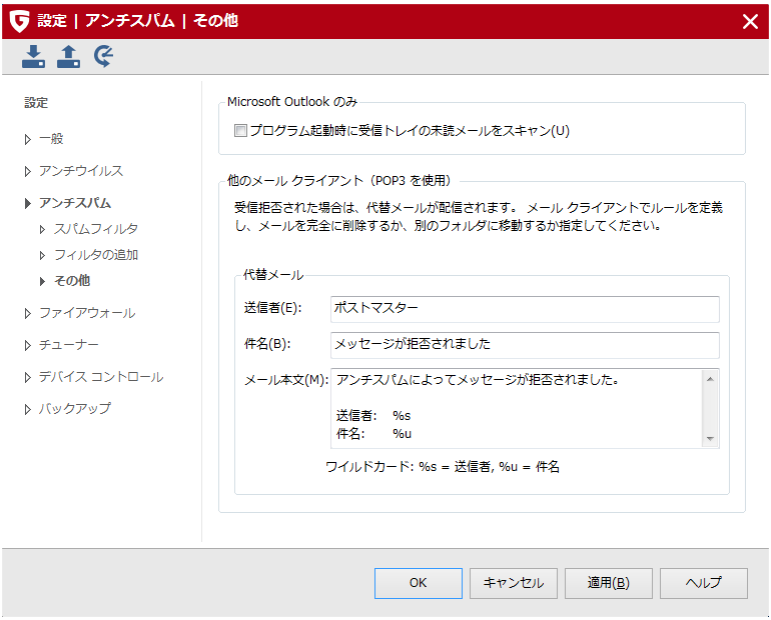
として定義します。例えば、英語のメールを受信することはないという場合には、英語をスパム言語として定義し、多数の英語で送られてくるメールを排除できます。メールを受け取ることはない言語と考えられる言語を選択すると、スパム検出精度はさらに向上します。

処理方法では、スパムと判断されたメールの処理方法を設定します。**メールの件名と本文に警告を挿入**にチェックを入れると、疑わしいメールの件名欄の件名の前に「スパム」または「注意」などの警告**（件名に追加する文字）**を挿入できます。

メールを拒否を有効にすると、メールプログラムはこの警告が件名欄に挿入されたメールを受信しません。スパムの疑いがある場合に、件名欄ではなく実際のメール本文の前にテキストを挿入することもできます**（本文中のメッセージ）**。

Microsoft Outlook を使用している場合（※Outlook Express または Windows Mail では不可）、スパムの疑いのあるメールを受信トレイ内の自由に定義できるフォルダに移動することができます**（メールをフォルダに移動）**。本製品は、**フォルダ名**の欄にフォルダを定義すれば直接フォルダを作成する機能を備えています。

その他
ここでは次の設定を行うことができます。



- **プログラム起動時に受信トレイの未読メールをスキャン**（Microsoft Outlook のみ）：Outlook を起動するとすぐに、受信トレイとそのサブフォルダにあるすべての未読メールをチェックします。

- **他のメールプログラム（POP3 を使用)**: POP3 で受信したメールは、POP3の仕様による制限で、すぐには削除できないことがあります。フィルタがメールの受信を拒否すると、このメールは下の代替テキストで書き換えられます。受信拒否メールの代替テキストは**「メッセージが拒否されました」**と表示されます。この代替テキストは自由に編集できます。件名とメール本文のテキストを、以下のワイルドカード (「%」記号に続けて小文字 1 文字) を使って自由に作成できます。

  %s　　送信者

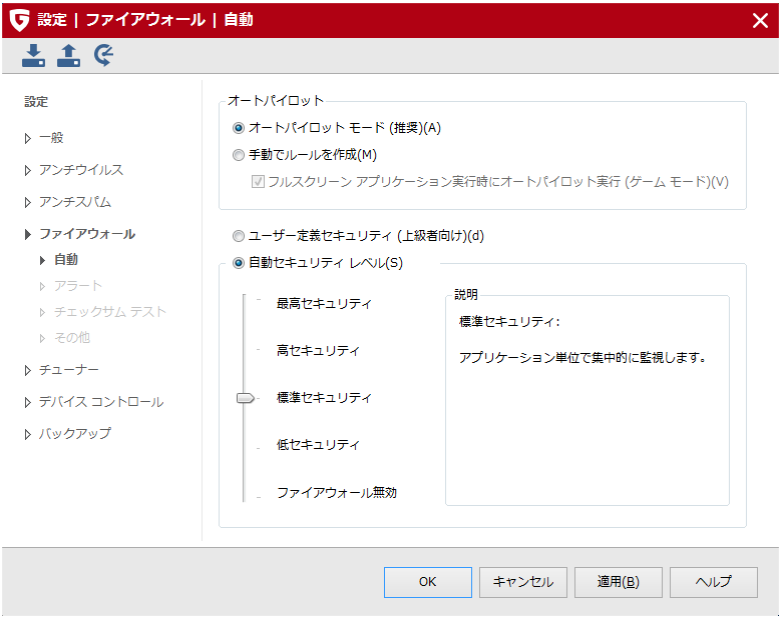
  %u　　件名

ここで設定したテキストを自動的に削除するルールをメールプログラムで設定できます。

ファイアウォール

自動

ファイアウォールは外部からの不正侵入からコンピュータを保護します。G Data のファイアウォールには、オートパイロットモードからマニュアルでのルール設定まで、初心者から上級者のニーズに応えることができる様々な設定が搭載されています。



ファイアウォール設定の**自動**は、以下の2つの領域から構成されています。

オートパイロット

ファイアウォールの作動方式を選択します。モードでは、**オートパイロットモード（推奨）**と**手動でルールを作成**から選択できます。

- **オートパイロットモード**: ファイアウォールが許可、またはブロックするアプリケーションを自動制御するので、ユーザーを煩わすことなく、コンピュータを最適に保護できます。（推奨設定）
- **手動でルールを作成**: ファイアウォールをネットワーク環境に合わせて設

定したり、特定のアプリケーションにオートパイロットモードを適用しない場合には、この設定を選択して、ルールを手動で作成します。

- **フルスクリーンアプリケーション実行時にオートパイロットを実行（ゲームモード）**：ゲームやフルスクリーン表示のアプリケーションを起動した際に、ファイアウォールが自動的にオートパイロットモードに切り替わるように設定します。この設定は、オートパイロットを通常は使用しない場合にのみ選択できます。

ユーザー定義セキュリティ

上級者向けの**ユーザー定義セキュリティ（上級者向け）**と G Data が定義した**自動セキュリティレベル**から選択できます。**自動セキュリティレベル**を使用すると、ネットワークセキュリティの専門知識がなくてもユーザーを煩わせることなく、ファイアウォールを環境に応じて設定できます。**自動セキュリティレベル**の設定は、非常にシンプルで、希望するセキュリティレベルにスライダを合わせて設定するだけです。設定レベルには以下の5種類があります。

- **最高セキュリティ**: ファイアウォールのルールを非常に細かく設定します。ネットワークの専門用語（TCP、UDP、ポートなど）に精通している必要があります。ファイアウォールは微小な不一致も検知するため、学習段階では非常に頻繁に確認が行われます。

- **高セキュリティ**: ファイアウォールのルールを細かに設定します。ネットワークの専門用語（TCP、UDP、ポートなど）に精通している必要があります。ファイアウォールが、学習段階で頻繁に確認が行われます。

- **標準セキュリティ**: ファイアウォールのルールをアプリケーションレベルで設定します。ネットワークの専門知識がなくても、ウィザードで簡単に設定できます。学習段階での確認頻度も最小限です。

- **低セキュリティ**: ファイアウォールのルールをアプリケーションレベルで設定します。ネットワークの専門知識がなくてもウィザードで簡単に設定できます。また、学習段階での確認もほとんどありません。このセキュリティレベルでも、着信する接続要求に対しては最高レベルのセキュリティが適用されます。

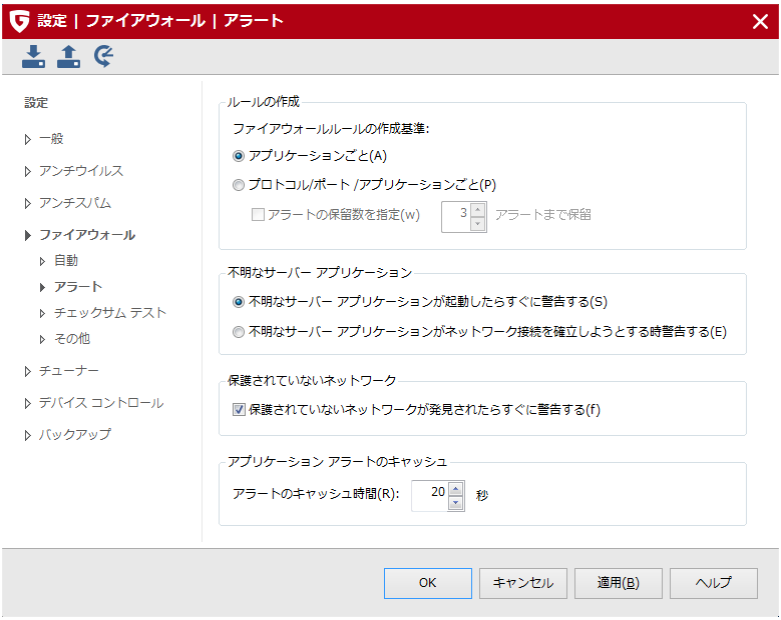
- **ファイアウォール無効**: ファイアウォールを無効にします。ファイアウォールを無効にしても、インターネットや他のネットワークとの接続は維持されます。外部からの攻撃やスパイウェアの防御が機能しなくな

るので、ファイアウォールを無効にする際は注意ください。

ファイアウォールを細かく設定するには、**ユーザー定義セキュリティ（上級者向け）**にチェックを入れます。この設定は、ネットワーク知識のある上級者にのみお勧めします。

アラート

ユーザー定義セキュリティ（上級者向け）にチェックを入れた場合、この領域の設定ができるようになります。アラートでは、このプログラムがインターネットやネットワークと接続を確立する時に、ファイアウォールがユーザーに確認を求めるタイミング、処理方法、確認の有無などを設定します。



ルールの作成

ファイアウォールがネットワークとの接続を検知すると、ポップアップが表示されます。この画面で、当該アプリケーションを許可／禁止するなどの処理方法を指定します。

- **アプリケーションごと**: 表示されたアプリケーションに対して、許可／拒否するポートおよびプロトコルを設定します。

- **プロトコル/ポート/アプリケーション**: ネットワーク接続を要求するアプリケーションに、要求されたポート（またはプロトコル）だけを使用したアクセスを許可します。このアプリケーションがさらに別のポート（またはプロトコル）でネットワーク接続を要求した場合は、追加ルールを作成するために、ユーザーに再度確認が行われます。

- **アラートの保留数を指定 ___ アラートまで保留**: 一部のアプリケーション（Microsoft Outlook など）は、ネットワークへのアクセス時に同一のリクエストを複数ポートへ送信したり、複数のポートやプロトコルを同時使用しています。このようなアプリケーションを使用している環境で**プロトコル / ポート / アプリケーションごと**を設定すると、ユーザーへの確認が複数回行われますが、特定回数以上、ユーザーへの確認があった場合は、**アプリケーションごと**に切換え、当該アプリケーションに対して許可／拒否を行うことができます。

不明なサーバーアプリケーション

ルールにないサーバーアプリケーションが起動した場合、もしくはサーバーアプリケーションが接続状態に入った時に、報告を発します。

保護されていないワイヤレスネットワーク

ファイアウォールが適切に機能するには、コンピュータが接続しているネットワークが認識され、かつファイアウォールによって監視されている必要があります。このため、通常はデフォルト設定の**保護されていないワイヤレスネットワークが発見されたらすぐに警告する**からはチェックを外さないでください。

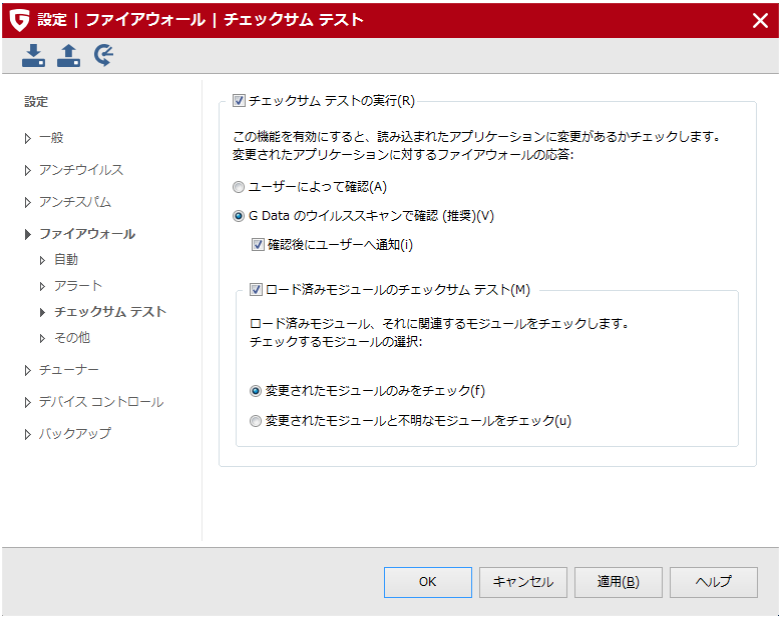
アプリケーションアラートのキャッシュ

ルールで定義されていない接続要求において、繰り返し行われる接続確認を特定の間隔で行うように設定できます。デフォルトでは、20秒に設定されています。

チェックサムテスト

チェックサムテストでは、ファイアウォールがネットワークアクセスを許可したアプリケーションに対して、ファイル容量などの判断基準から構成されるチェックサムを使い、その信頼性をチェックします。アプリケーションのチェックサムが一致しない時は、アプリケーションが改変された可能性があるので、アラートが発せられます。

チェックサムテストの実行: アプリケーションに加えてモジュール（例：DLL）も監視します。モジュール変更や新たなモジュールのロードは頻繁に行われるため、モジュール変更と不明なモジュールを完全に管理するのは手間がかかります。モジュールチェック機能は非常に高レベルのセキュリティが必要な場合にのみ使用してください。



その他
他にも以下のような設定も可能です。

デフォルトで使用するウィザードの種類

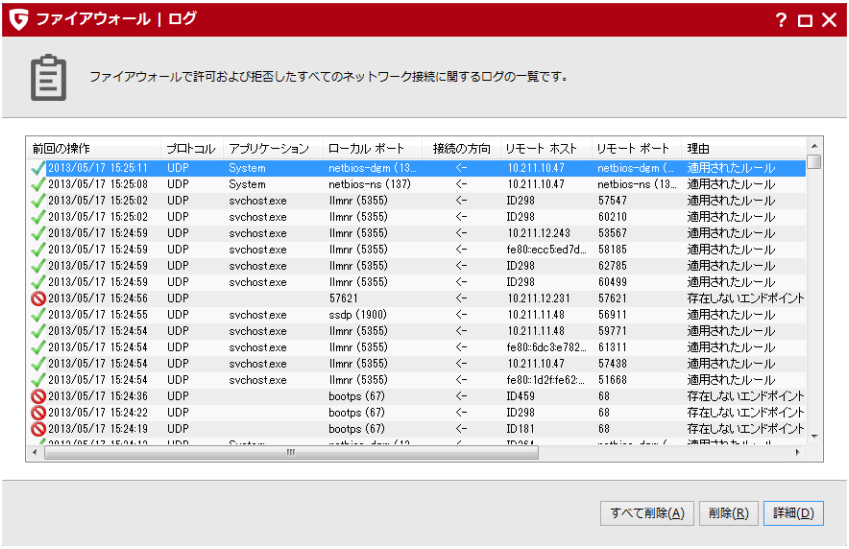
新規ルールの生成方法を**ルールウィザード**もしくは**詳細設定ダイアログ**から選択します。**詳細設定ダイアログ**は上級者向けの設定モードです。

プログラム起動時のチェック

アプリケーション起動の度に、ファイアウォールが不明なサーバーアプリケーションをチェックします。この設定は、クローズドネットワークを除くすべてのネットワーク環境で有効にしておく事をお勧めします。

接続ログの保存

ファイアウォールのログを保管する期間を設定します。期間は1～60時間の中から選択できます。ログは、ファイアウォール領域に移動して、ログアイコンを押すと表示できます。


ファイアウォール | ログ
ファイアウォールで許可および拒否したすべてのネットワーク接続に関するログの一覧です。
前回の操作 プロトコル アプリケーション ローカル ポート 接続の方向 リモート ホスト リモート ポート 理由
2013/05/17 15:25:11 UDP System netbios-dgm (13... <- 10.211.10.47 netbios-dgm (... 適用されたルール
2013/05/17 15:25:08 UDP System netbios-ns (137) <- 10.211.10.47 netbios-ns (13... 適用されたルール
2013/05/17 15:25:02 UDP svchost.exe llmnr (5355) <- ID298 57547 適用されたルール
2013/05/17 15:25:02 UDP svchost.exe llmnr (5355) <- ID298 60210 適用されたルール
2013/05/17 15:24:59 UDP svchost.exe llmnr (5355) <- 10.211.12.243 53567 適用されたルール
2013/05/17 15:24:59 UDP svchost.exe llmnr (5355) <- fe80:ecc5:ed7d... 58185 適用されたルール
2013/05/17 15:24:59 UDP svchost.exe llmnr (5355) <- ID298 62785 適用されたルール
2013/05/17 15:24:59 UDP svchost.exe llmnr (5355) <- ID298 60499 適用されたルール
2013/05/17 15:24:56 UDP 57621 <- 10.211.12.231 57621 存在しないエンドポイント
2013/05/17 15:24:55 UDP svchost.exe ssdp (1900) <- 10.211.11.48 56911 適用されたルール
2013/05/17 15:24:54 UDP svchost.exe llmnr (5355) <- 10.211.11.48 59771 適用されたルール
2013/05/17 15:24:54 UDP svchost.exe llmnr (5355) <- fe80:6dc3:e782... 61311 適用されたルール
2013/05/17 15:24:54 UDP svchost.exe llmnr (5355) <- 10.211.10.47 57438 適用されたルール
2013/05/17 15:24:54 UDP svchost.exe llmnr (5355) <- fe80:1d2f:fe62... 51668 適用されたルール
2013/05/17 15:24:36 UDP bootps (67) <- ID459 68 存在しないエンドポイント
2013/05/17 15:24:22 UDP bootps (67) <- ID298 68 存在しないエンドポイント
2013/05/17 15:24:19 UDP bootps (67) <- ID181 68 存在しないエンドポイント
すべて削除(A)
削除(R)
詳細(D)

ログ

本製品に搭載されている各機能には、保護などを行った際の動作を記録、確認するためのログ機能が搭載されています。

アンチウイルスのログ

アンチウイルスのログ領域には、ウイルスからの保護状況や、ワクチンのアップデート状況が記録されます。

列見出しの **開始時刻**、**種類**、**内容** もしくは**ステータス**をクリックすると、ログを並び替えることができます。**「名前を付けて保存」**では、ログをテキストファイルに保存し、 **「印刷」**ではログを印刷できます。ログを削除するには、対象を選択してから、**「削除」**ボタン（もしくはキーボードの **Delete キー**）を押してください。

ファイアウォールのログ

ファイアウォールのログ領域には、ファイアウォールで許可および拒否されたネットワーク接続とインターネット接続がすべて記録されます。

任意の列の見出しをクリックすると、その項目に従って並び替えができます。また、行を選択して**「詳細」**をクリックすると、その接続についての詳しい情報が表示されます。ログの保存期間を変更したい場合は**設定 | その他**の項に従って変更してください。

フィルタリングのログ

フィルタリングのログ領域では、管理者は各ユーザーの接続履歴、拒否されたコンテンツの内容やブロックした理由などの情報を確認できます。詳しくは**設定:ログ**の項をご覧ください。

「ログを削除」をクリックすると、ログは消去されます。

FAQ: ブートスキャン

本製品には、Windows 起動前にスキャンを実行できる**ブートスキャン**機能が搭載されています。 ブートスキャンは、本製品をインストールする前からコンピュータに感染し、本製品のインストールを妨害する可能性のあるウイルスの駆除をするのに役立ちます。

> **ブートとは**: コンピュータの電源を入れると、通常は自動的に Windows OS が起動します。このプロセスを「ブート」と呼びます。このプロセスでは Windows OS だけでなく代わりに別のOSを自動的に起動させることもできます。本製品のブートメディアを使用すると、ブートの際、 Windows の代わりに専用OSでコンピュータを起動することができ、そのOS上でウイルススキャンを行う事ができます。

ブートスキャンの準備

ブートスキャンは、本製品をインストールする前からコンピュータに感染し、本製品のインストールを妨害する可能性のあるウイルスの駆除をするのに役立ちます。このブートスキャン機能は、Windows を使用せずにコンピュータをブートメディアから起動してスキャンを行う機能です。

CD/DVD からのブート: コンピュータが、ブートCD/DVD から起動できない場合は、以下の手順をお試しください
（コンピュータの操作に慣れた上級者が設定されることをお勧めします）:

1. コンピュータをシャットダウンします。
2. コンピュータを起動し、**BIOS 設定画面**を表示します。通常 BIOS 設定を行うには、コンピュータの起動（= ブート）時に **Delete** キー（F2 キーまたは F10 キーの場合もあります）を押します。
3. 次に、BIOS 設定画面で、ブートデバイスの優先順位を変更します。BIOS の各設定項目をどのように変更するかはコンピュータによってさまざまですので、コンピュータの取扱説明書をお読みください。変更後のブート順は **CD/DVD: , C:** にします。具体的には、CD/DVD ドライブを [**1st Boot Device**] （第1ブートデバイス）とし、Windows OS がインストールされているハードディスクパーティションを [**2nd Boot Device**] （第2ブートデバイス）とします。

4 変更を保存して、コンピュータを再起動します。これでブートメディアからブートできる状態になりました。

ブートスキャンを中断するには: 通常、コンピュータに起動中にブートメディアが挿入されているとブートスキャンの画面が表示されます。Windows 起動画面を表示したい場合は、ブートスキャンのメニュー画面で矢印キーを使い、**Microsoft Windows** を選択し、**Enter** キーを押します。すると、Windows が通常通り起動します。

USBメモリからのブート: USBメモリのブートメディアからブートする場合も、CD/DVDと同じ要領で 1st Boot Device として認識されるように設定してください。それでも起動時に認識されない場合は、コンピュータの起動時に**ブートメニュー**を使用し、対象のUSBメモリを選択して、ブートを行ってください。**（ブートメニューの表示方法はコンピュータによって異なりますので、コンピュータの取扱説明書などをご確認ください）**

ブートスキャンの流れ

ブートスキャンを実行するには、以下の手順に沿って行ってください:

1 **CD版製品でのブートスキャン**: **製品CD** をCDトレイに挿入します。表示された起動ウインドウで、**「キャンセル」** をクリックし、コンピュータをシャットダウンします。

ダウンロード版製品でのブートスキャン: 本製品の**「ウイルス対策」**画面にある、**「ブートメディアを作成」** を選択して、ブートCD を作成します。作成が完了したら、作成したブートCD をCDトレイに挿入して、コンピュータをシャットダウンします。
※ブートCDの挿入後に起動画面が表示された場合は、**「キャンセル」**をクリックしてコンピュータをシャットダウンします。

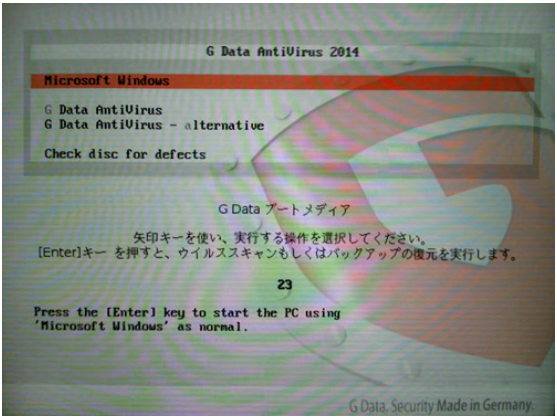
メモ: Windows XP 上では、ブートCDの作成時に**「IMAPI 2.x がインストールされていません」**というメッセージが表示されることがあります。これは、古いOSでデータをメディアにコピーするために必要な Microsoft の更新プログラムです。Microsoftのサイトからダウンロードしてインストールしてください。

USBメモリを利用したブートスキャン: 本製品の**「ウイルス対策」**画

面にある、**「ブートメディアを作成」** を選択して、ブートUSB を作成します。作成が完了したら、作成したブートUSB をPCに差し込み、コンピュータをシャットダウンします。
※ブートCDの挿入後に起動画面が表示された場合は、**「キャンセル」**をクリックしてコンピュータをシャットダウンします。

注意: ブートUSBから起動する場合は、コンピュータがUSBメモリからブートできる状態でなければなりません。多くの場合は、起動時にコンピュータのブートメニューを使用する事でブート可能です。詳しい解説は、**ブートスキャンの準備**の項の**USBメモリからのブート**を確認ください。

2 コンピュータを再起動します。**G Data ブートスキャン**のスタートメニューが表示されます。



3 矢印キーで **G Data AntiVirus(もしくはG Data BootMedium)** を選択し、**Enter** キーで確定します。そうすると、自動的に Linux OS が起動し、ブートスキャン用画面が表示されます。

メモ: プログラム画面が正常に表示されない場合には、コンピュータを再起動して **G Data AntiVirus - Alternative** を選択してください。

メモ: TotalProtection を使用している場合はこの画面の後に、アンチウイルスを起動するか、バックアップの復元機能を起動するか、を選

択する画面が表示されます。

4 **ワクチン**を更新するよう促されます。

5 **「はい」**をクリックして更新を実行してください。インターネットを介してデータが更新されると、**「更新できました」**というメッセージが表示されます。**「閉じる」**をクリックして更新画面を閉じます。

メモ: 自動インターネット更新機能は、IP アドレスを自動割当機能（DHCP）を持つルータを使用している場合にのみ、利用できます。インターネット更新が利用できなくても、古いワクチンを利用して、ブートスキャンを実行できます。ただし、この場合には、本製品のインストール後できるだけ早いうちに、更新したワクチンを使って、ブートスキャンを実行してください。

6 プログラムの画面が表示されます。スキャン領域で**「コンピュータ」**をクリックすると、コンピュータ全体のスキャンが開始されます。一般的に、コンピュータ全体のスキャンを行った場合は、スキャン終了まで数時間以上の時間を要します。一部のフォルダのみのスキャンで十分な場合は、**「ファイルとフォルダ」**で対象のフォルダを選択してスキャンすると、スキャン時間も短く済み、効率的です。

7 **ウイルスが検出されたら**、本製品が提案する処理方法から適当なものを選択して、ウイルス駆除を行ってください。ウイルスを駆除できたら、オリジナルファイルが再び使用可能な状態になります。 なお、ファイルがシステムファイルや重要なファイルと思われる場合は、削除しないことをお勧めします。

メモ: 削除を選択する場合は、対象のファイルが削除されてもシステムに問題を引起さないことを確かめてから、操作を実行してください。

8 ウイルススキャンが完了したら、画面右上の X マークをクリックして、終了してください。

9 ドライブのトレイが開いたら、**ブートCD** を取り出します。（**USBメモリ** を使用してブートスキャンしている場合は、コンピュータのUSBスロットに差し込まれているUSBメモリを抜きます。）

10 コンピュータを再起動し、通常通り Windows OS を起動します。
（CDやUSBメモリが挿入されている場合は、すぐに取り出してください）

FAQ: 各種機能について

G Data アイコン

本製品の保護機能が有効に機能しているかどうかは、タスクバー上の G Data アイコンで確認できます。

このアイコンが表示されている時は、G Data によるセキュリティ保護が有効で、コンピュータが適切に保護されていることを意味しています。

警告マーク付きのアイコンが表示される時には、セキュリティ保護が有効になっていないことを意味しています。このアイコンは、ウイルスガードを無効にしたり、セキュリティ保護に問題がある場合に表示されます。

このアイコンが表示されている時は、本製品がインターネットから更新ファイルをダウンロードしています。

G Data アイコン上で右クリックをすると、右クリックメニューが表示されます。右クリックメニューからは、ユーザーがよく使用する操作が選択できます。

画像はトータルプロテクションのものです。

ここでは以下の操作を選択できます:

- **G Data（製品名）を起動**: 本製品プログラムのセキュリティセンターを

呼び出します。セキュリティセンターに関する詳細は、セキュリティセンターを参照してください。

- **ウイルスガードを無効にする**: ウイルスガードの有効／無効を切り替えます。大容量のファイルをコピーしたりする際にウイルスガードを無効にすると処理がより高速に行われますが、ウイルスガードを無効にする期間は最小限に抑えてください。またウイルスガードが無効な間は、インターネットやスキャン未実行のメディア（CD/DVDやUSBメモリなど）と接続しないようにしてください。

- **ファイアウォールを無効にする**: ファイアウォールが搭載されている製品では、右クリックメニューからファイアウォールの有効／無効を切り替えることができます。インターネット接続環境では、ファイアウォールを無効にした後も、コンピュータは引き続きインターネットに接続されます。このとき外部からの攻撃から保護されませんので、ファイアウォールを無効にする際は注意してください。

- **オートパイロットを無効にする**: ファイアウォールのオートパイロット機能の有効／無効を切り替えます。オートパイロットはファイアウォールの処理をユーザーに代わって自動的に判断する機能で、これを無効にすると、ネットワーク接続についてユーザーへ確認が行われるようになります。通常はオートパイロットを有効にした状態で利用することをお勧めします。

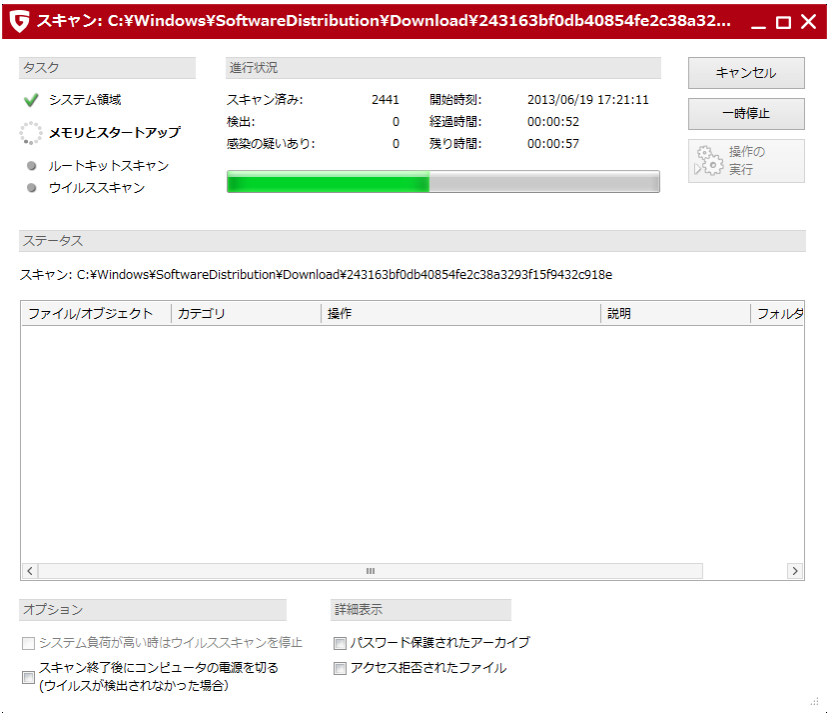
- **ワクチンを更新**: 今すぐにワクチン更新を手動実行します。コンピュータの適切な保護には、ワクチン更新は非常に重要です。ワクチン更新は通常、自動更新に設定しておいてください。インターネット更新に関する詳細は、更新の項を参照してください。

- **データセーフを開く**: トータルプロテクションを使用している場合は、データセーフ作成後にここから任意のデータセーフを開く事ができます。

- **統計情報**: メール、ウェブ、ウイルスガードなどのスキャン統計を確認できます。

ウイルススキャンの流れ

ウイルススキャンは、コンピュータ上のマルウェアをスキャンする機能です。ウイルススキャン中にウイルスが検出されると、検出されたウイルスへの対処方法を選択できます。



検出されたウイルスには、それぞれの検出ごとに、削除、駆除、隔離といった対処が可能です。

1 ウイルススキャンを開始します。ウイルススキャンの開始方法は、アンチウイルスの各項目を参照してください。

2 コンピュータ上でスキャンが始まると、スキャンのステータス情報を表示する画面が開きます。

画面上部のステータス表示バーには、スキャンの進捗状況が表示されます。ウイルススキャンのプロセスに関する設定は、スキャン中に行

うことができます。設定できる項目は次の通りです:

- **システム負荷が高い時はウイルススキャンを停止**: ユーザーがコンピュータで作業を行っている間は、ウイルススキャンを自動的に停止します。
- **スキャン終了後にコンピュータの電源を切る**: ウイルススキャン終了後に、コンピュータが自動的にシャットダウンします。例えば、一日の作業終了時にスキャンを行う場合などに使用すると便利です。
- **パスワード保護されたアーカイブ**: アーカイブがパスワードで保護されている場合、このアーカイブはスキャンされません。ここにチェックを入れると、スキャンできなかったパスワード保護されたアーカイブを表示します。これらのアーカイブにウイルスが潜んでいたとしていても、解凍しない限り、ウイルスがシステムに感染する可能性はありません。
- **アクセス拒否されたファイル**: Windowsでは、通常、アプリケーションが自身の動作のために使用するファイルを、そのアプリケーションの実行中にスキャンできません。スキャン実行中は、可能な限り、他のプログラムを実行しないようにしてください。ここにチェックを入れると、スキャンできなかったデータが表示されます。

3a ウイルススキャン結果が画面に表示されます。ウイルスが検出されなければ、**「閉じる」**をクリックして画面を閉じます。

3b **ウイルスが検出された場合**は、**「操作の実行」**をクリックして感染ファイルの処理を行います。

デフォルト設定（設定 | アンチウイルス | ウイルススキャンで、何も変更しなかった場合）では、感染ファイルからウイルスを駆除します。ウイルスを駆除に成功したファイルは再び普通に使用してもコンピュータに支障をきたしません。

駆除できない場合には、ファイルは隔離領域に移動されます。隔離されたファイルは、暗号化して保存されるので、コンピュータに問題を引起すことはありません。この感染ファイルが必要にな場合は、隔離領域から元の場所に戻して使用できます。

3c 感染ファイルやオブジェクトが、必要か不要がを判別できる場合には、スキャン結果 1 件ごとに操作を実行することもできます。

スキャン結果一覧の**「操作」**領域で、感染ファイル 1 件ごとに処理方法を決めます。

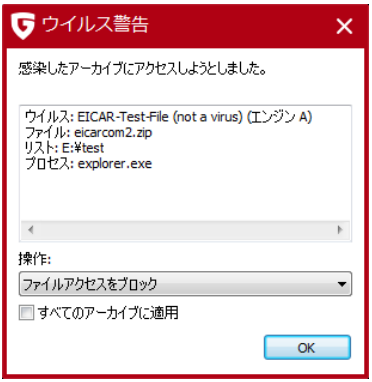
- **ログを残すのみ**: 感染したファイルをログとして記録します。感染ファイルのウイルス駆除やファイル削除はされません。※ウイルスをログに残すだけの場合、ウイルスは活動を続けるため危険です。
- **ウイルス駆除（不可能な場合はログを残すのみ）**：感染ファイルからウイルスを駆除できない場合には、ファイルを検出時のままの状態でログに残し、このログを基に後で処理方法を決めることができます。※ウイルスをログに残すだけの場合、ウイルスは活動を続けるため危険です。
- **ウイルス駆除（不可能な場合は隔離）**：感染ファイルからウイルスを駆除できない場合には、ファイルを検出時のままの状態でログに残し、**隔離**します（推奨設定）。隔離に関する詳細は、**隔離されたファイル**を参照してください。
- **ウイルス駆除（不可能な場合はファイルを削除）**：感染ファイルからウイルスを駆除できなかった場合は、ファイルを削除します。この処理方法は、コンピュータ上に重要なデータが無い場合にのみ選択してください。※感染ファイルを完全に削除すると、場合によっては、Windows の動作に影響を与える可能性があります。対象のファイルが、削除しても問題ないファイルの時にのみ、選択してください。
- **ファイルを隔離**: 感染ファイルを暗号化して、**隔離領域**に移動します。隔離領域に移動した感染ファイルは、後で修正できるように暗号化して保管され、有害な活動ができないように暗号化されます。隔離に関する詳細は、**隔離されたファイル**を参照してください。
- **削除**: ファイルを削除します。※感染ファイルを完全に削除すると、場合によっては、Windows の動作に影響を与える可能性があります。対象のファイルが、削除しても問題ないファイルの時にのみ、選択してください。

「操作を実行」をクリックすると、検出されたウイルスごとに、ユーザーが設定した処理が行われます。

これでスキャン終了です。ログを残すのみにしていた検出がある場合は、マルウェアはまだコンピュータに残った状態になっていますので、ご注意ください。

ウイルス検出時の対応

ウイルスまたは他の不正プログラムが発見された場合、感染ファイルを以下の方法で処理できます。



感染ファイルにアクセスしようとした際に表示されるダイアログで、以下の処理方法を選択できます:

- **ファイルアクセスをブロック**: 感染したファイルへのアクセスをブロックします。感染ファイルのウイルス駆除やファイル削除はされません。※一時的にアクセスはブロックされますが、ウイルスはコンピュータに残るため危険です。
- **ウイルス駆除（不可能な場合はアクセスをブロック）**: 感染ファイルからウイルスを駆除できない場合には、ファイルへのアクセスをブロックします。※一時的にアクセスはブロックされますが、ウイルスはコンピュータに残るため危険です。
- **ウイルス駆除（不可能な場合は隔離）**: 感染ファイルからウイルスを駆除できない場合には、ファイルを検出時のままの状態でログに残し、隔離します（推奨設定）。隔離に関する詳細は、隔離されたファイルを参照してく

ださい。

- **ファイルを隔離**: 感染ファイルを暗号化して、**隔離領域**に移動します。隔離領域に移動した感染ファイルは、後で修正できるように暗号化して保管され、有害な活動ができないように暗号化されます。隔離に関する詳細は、隔離されたファイルを参照してください。

- **感染ファイルを削除**: ファイルを削除します。※感染ファイルを完全に削除すると、場合によっては、Windows の動作に影響を与える可能性があります。対象のファイルが、削除しても問題ないファイルの時にのみ、選択してください。

  メールボックスの隔離に関しての注意: ※電子メールのメールボックス用のアーカイブは隔離しないでください。メールボックスのアーカイブ（**拡張子.pst のファイルなど**）が隔離されると、メールプログラムはメールデータにアクセスできなくなり、メールプログラムは適切に機能しなくなります。

ファイアウォールアラート

オートパイロットを使用せずに**手動でルールを作成**モードを使用すると、未知のアプリケーションやプロセスがネットワークへのアクセスを試みた際に、アクセスの許可／拒否について、ユーザーに確認が行われます。

確認は、画面の右下からのポップアップで行われます。このポップアップでは、ユーザーは、アプリケーションに対して、ネットワークアクセスを**一時的に許可/拒否**または**常に許可/拒否**という処理方法から選択できます。アプリケーションにアクセスを**常に許可/拒否**すると、操作がアクセスするネットワークのルールセットに取り込まれ、以降はアラートが表示されなくなります。

ネットワークのルールセットに取り込まれたルールは、**ルールセット**の**コメント**で**アラートにより作成**と表示されます。

アラートのポップアップ画面では、次の選択操作が可能です:

- **常に許可**: アプリケーションに対して、表示されたネットワーク内でのネットワークまたはインターネットへのアクセスを常に許可します。**ルールセット**領域には、アラート経由で作成されたルールとして表示されます。
- **一時的に許可**: アプリケーションに対して、ネットワークアクセスを 1 回だけ許可します。アプリケーションが再度ネットワークへアクセスを試みると、ファイアウォールが改めてアクセスの可否を問い合わせます。
- **常に拒否**: アプリケーションに対して、表示されたネットワーク内でのネットワークまたはインターネットへの接続を常に拒否します。**ルールセット**領域には、アラート経由で作成されたルールとして表示されます。
- **一時的に拒否**: アプリーションに対して、ネットワークアクセスを 1 回だけ拒否します。アプリケーションが再度ネットワークへアクセスを試みると、ファイアウォールが改めてアクセスの可否を問い合わせます。

アプリケーションが利用しようとしているロトコル、ポート、IPアドレスなどの情報もここのアラート画面で確認できます。

ウイルススキャンで「not-a-virus」が表示される

「not-a-virus」 と表示されるファイルは、ファイル自身は不正機能を持っていませんが、ある状況においては攻撃者によって不正利用され、コンピュータに危害を加えられる可能性があるアプリケーションです。

not-a-virus カテゴリには、キー配列自動変更ツール、IRCクライアント、FTPサーバー、プロセス作成（または隠す）ツールなどあります。

アンインストールの方法

本製品をアンインストールする場合は、以下の手順でアンインストールが可能です。

- **Windows 8**: スタート画面（Modern UI）から、本製品のアイコンを右クリックし、画面下の **［アンインストール］** を選択します。表示された **［プログラムと機能］** ウインドウから、本製品を選択し、 **［アンインストール］** をクリックしてアンインストールを実行します。
- **Windows Vista**, **Windows 7**: Windows タスクバーで **[スタート]** （通常はディスプレイの左下に配置）をクリックし、**[コントロールパネル]** を選択します。 そこで **[プログラム] > [プログラムのアンインストール]** を選択します。表示されたリストから 本製品を選択し、**[アンインストール]** をクリックしてアンインストールを実行します。
- **Windows XP**: Windows タスクバーの **[スタート]** をクリックして **[設定] > [コントロールパネル] > [プログラムの追加と削除]** を選択します。表示された **[プログラムの追加と削除]** ウインドウから、本製品をマウスで選択します。そして **[変更と削除]** をクリックしてアンインストールを実行します。

隔離済みファイルが**隔離**領域に残っていると、アンインストール中に、これらファイルを削除するかどうかを確認されます。隔離ファイルを削除しない場合は、当該ファイルは暗号化されてコンピュータ上に保存され、アンインストール後もコンピュータ内に残ります（これらのファイルは本製品を再インストールしないと使用できません）。また、アンインストール中に、**設定とログ**を削除するかどうかについても確認されます。これらのファイルを削除せずにコンピュータに残しておくと、ソフトウェアを再インストールした場合、保存されたログと設定が再び使用できるようになります。

「終了」をクリックすると、アンインストールを終了します。これでソフト

ウェアがシステムから完全にアンインストールされます。

FAQ: ライセンスについて

複数台用ライセンスを所有している場合

複数台用ライセンスをご購入いただくと、取得したライセンスと同数のコンピュータに 本製品をインストールして使用できます。1 台目のコンピュータへのインストールとインターネット更新が終了すると、メールでアクセスデータが送信されます。2 台目のコンピュータにもソフトウェアをインストールする時には、1台目の登録の際に発行されたユーザー名とパスワードを入力します。3 台目以降のコンピュータにもこの作業を繰り返します。

複数台用ライセンスの製品を複数のコンピュータで使用する際は、初回登録時に発行されたインターネット更新用の**アクセスデータ**（ユーザー名とパスワード）を、すべてのコンピュータで使用します。手順は以下のとおりです。

1. 本製品を起動します。
2. セキュリティセンター画面で**「前回のワクチン更新」**をクリックし、プルダウンメニューから**「今すぐワクチン更新」**をクリックします。
3. 表示されるウィンドウに、G Data から送られてきたメールで送信されたアクセスデータを入力します。**「OK」**をクリックすると、更新ができるようになります。

ライセンスの期限が切れた場合

ライセンスの期限切れが近づくとポップアップのメッセージでお知らせします。このポップアップメッセージをクリックすると、ダイアログが開き、ここから更新の手続きを行うことができます。

メモ: 更新手続きは **G Data ウェブサイト** からも可能です。

コンピュータを買い替えたり、クリーンインストールした場合

コンピュータを買い換えたり、クリーンインストールした場合は、本製品をコンピュータにインストールし、初回登録時に G Data から送付されたアクセスデータを入力します。アクセスデータの入力は、**インストール**もしく**更新**の項を参照してください。

> **メモ**: ライセンスの移行には回数制限が設定されています。この回数を超えた場合は、更新期限が有効でも更新がロードできなくなりますので、ユーザーサポートに問い合わせください。

データ保護に関する声明

本ソフトウェアのデータ保護に関する声明

G Data製品には、特定条件下においてデータをG Dataのクラウドサーバーへ送信する保護コンポーネントが含まれています。保護コンポーネントのコア機能を正常に機能させるために必要な特定データは、常に同サーバーへ送信されます。保護コンポーネントの１つ、ウェブ保護には、ウェブサイトのアドレス送信が必須となります。また、別の保護コンポーネント、バンクガードでは、新種のバンキング系トロイの木馬の特定・削除のために、チェックサムの送信が必要となります。更に、ふるまい検知（ビヘイビアブロッカー）の機能は、クラウドからの情報を取得することにより、コンピュータをより効果的に保護できますが、これには、不審なファイルに関する特定の情報をクラウドサーバーへ送信する必要があります。

また、送信されるデータは、他のコンポーネントにおいても重要な意味を持っています。ユーザー様から送信されたデータは、G Dataのセキュリティラボで有害なファイルを検証や挙動の分析に使用されます。検証結果は、G Dataの保護コンポーネントの改善やG Data製品のユーザーへの有害プログラムに関する情報やその影響を提供します。詳細は、マルウェア情報イニシアチブ（MII）のデータ保護に関する声明をご覧ください。なお、MIIへの参加は任意です。MIIへの参加を無効化しても、G Dataによる保護メカニズムは、その効果を制限されません。

重要：　これらの機能で収集される情報には、個人情報は含まれません。また、取得した情報を使って個人の特定を行うことはありません。

・ウェブ保護によるデータ収集

G Data ウェブ保護とは?

インターネットには、数多くの有害サイトや詐欺サイトが存在しています。これらのサイトは、マルウェア配布や適切な保護が施されていないコンピュータを感染させるための感染経路（Drive-By-Infection）として使われており、個人情報を盗み出したり（例： PaypalやFacebookのサイトフィッシング）、スキャムなどの詐欺として使用されている可能性があります。G Dataは、有害サイトへのアクセスを遮断するブラックリストを独自に管理・保守しています。G Dataウェブ保護は、次の2種類のテクノロジーがベースとなっています。

1. HTTPスキャン。この機能は、既知の有害コードがないか、ウイルススキャナでスキャンしてHTTPトラフィックをチェックする機能です。有害コードが見つかった場合、G Dataが警告を発します。なお、警告が表示された場合、ユーザーが安全性に関する判定情報を、任意で送信できるケースがあります。

2.フィッシング保護。この機能は、リクエストされたアドレスがフィッシングサイトではないか、G Data が管理・保守するブラックリストと照合し、フィッシングサイトであった場合は警告を発する機能です。このURLブラックリストには、無数の有害サイトや詐欺サイトの情報が保存されています。なお、フィッシング警告が表示された場合、ユーザーが安全性に関する判定情報を、任意で送信できるケースがあります。

収集される情報の種類は?

リクエスト先のウェブサイトがG DataのURLブラックリストに存在するかチェックするため、ウェブサイトのアドレスをクラウドサーバーに送信します。

収集された情報の使用方法は?

リクエスト先のアドレスは、G Dataのデータベースに保存されますが、リクエスト送信元のユーザーもしくはPC情報は保存されません。ウェブサイトのアドレスは、まずG Dataの分析システムに転送され、次のステップで、有害もしくは不審な構成部分をチェックします。不審なウェブサイトのアドレスは、G Dataセキュリティラボの分析システムに転送されます。分析によって不審サイトと確認された場合は、このサイトはブラックリストに追加されます。

G Dataのクラウドサーバーとリクエスト送信元コンピュータの間の接続中は、送信元コンピュータのIPアドレスが送信されますが、通常、このIPアドレス情報はG Data側では保存されません。ウェブサイトがブロックされた場合は、IPアドレスをもとに国情報を識別しますが、IPアドレスは識別後に破棄します。そのため、G Data側でリクエスト送信元の個人を特定することはできません。

・G Data バンクガードによるデータ収集

G Data バンクガードとは?

G Data バンクガードは、ブラウザのメモリ領域が破損状況やマルウェアによる改竄など、ブラウザが暗号化された情報の送信に使用するシステムライブラリを監視する機能です。G Data バンクガードがこの領域への攻撃を検出すると、保護メカニズムが作動し、攻撃されたブラウザを通常ステータスに戻します。その後、攻撃を引き起こした有害ファイルをシステムから見つけ出し、除去します。

収集するデータの種類は?

ブラウザのメモリが攻撃された場合、次の情報が送信されます 。

バージョン番号

- G Data 製品および同コンポーネント
- ブラウザおよび同コンポーネント
- OS情報

チェックサム

- 攻撃元および攻撃に関わったファイル
- 削除されたファイル

匿名 GUID

- 発生した事象を特定のコンピュータを関連付けるため、コンピュータのGUID情報を取得します。なお、GUIDは同一の情報が存在する可能性は非常に低く、GUIDからコンピュータの場所や個人の特定はできません。

攻撃時のアクティビティ情報

- 攻撃を特定マルウェアに関連付けるため、攻撃種類をもとにマルウェアを特定するフィンガープリントを取得します。フィンガープリントはシステムライブラリの呼び出しに基づくもので、これには個人情報は含まれません。

- 各システムライブラリで危険にさられている機能の名称

マルウェア除去時のアクティビティ情報

- 削除されたレジストリエントリ

- 削除時: ルートキットの種類（例： Watchdog/Versteck via Hook)

収集された情報の使用方法は?

バージョン番号は、発生した事象とプログラムバージョンを関連付けるために使用します。これは、エラー発生数の減少と脆弱なシステムの特定に役立ちます。

関連付けられたファイルのチェックサムは、G Dataのデータベース内の有害ファイルとの照合やさらに詳しい分析を行う上で、役立ちます。G Dataが保しない新たな脅威が発生した場合、この脅威は、リクエストリストへと入れられます。そして、次にこの脅威へのリクエストが確認された場合、実際にファイルが転送されます。このリクエストは、同じコンピュータから複数回送信されることはほぼありません。このリクエストは、実行可能なファイルの場合にのみ、送信されます。ドキュメント、画像、またはその他の個人情報を含むファイルなどは、送信されません。

フィンガープリントで、マルウェアを特定の系種に識別できます。同じ系種に属するマルウェアは同様の手法を用いて駆除できます。

クラウドサーバーとリクエストされたコンピュータ間の接続中は、リクエストされたコンピュータのIPアドレス情報が取得されますが、これは保存されません。ウェブサイトが有害と判定された場合、このIPアドレスを用いて、リクエスト元の国情報を取得します。このプロセスの後、IPアドレスは破棄されるため、G Data でユーザー情報の詳細を特定することはできません。

攻撃時のアクティビティ、更に攻撃に関わったり、削除されたファイルおよびレジストリエントリの情報は、削除ルーチンの分析・開発に役立ちます。これらのデータを使うと、新たな脅威や攻撃に迅速に対応できるようになります。

特定のデータは統計に使用されます。系種別の出現頻度などはG Dataのホワイトペーパーやマルウェアレポートで使用されます。また、これらの情報は、作業プロセスの優先度の決定や自動化にも使われています。

・ふるまい検知およびファイルクラウドセキュリティによるデータ収集

ふるまい検知とは?

ふるまい検知は、コンピュータ上のすべてのアクティブなプログラムによる不審な動きを監視する機能です。ふるまい検知では、プログラムによる挙動がすべてポイントで計算され、特定の値を超えると、当該プログラムを終了に導きます。特定の条件下においては、ふるまい検知は不審なファイルのチェックサムをG Dataのサーバーへと送信し、既知のマルウェアファイルと照合します。チェックサム送信の条件は、プログラムのダウンロード時、プログラムの初回起動時、プログラムによるある程度の不審な動きが実行された場合などがあります。ファイルが有害であると判断された場合は、プログラムの実行を中止するかどうか、ユーザーに確認します。

収集するデータの種類は?

ファイルをチェックする場合、チェックサム情報を取得し、サーバーに送信します。更に、ふるまい検知が有害度評価のために取得されたパラメーター（例: 有害度（0-1）、評価したルールのID番号）が送信されます。ファイルが有害と判定された場合、プログラムの呼び出しパラメーターが取得されます。警告メッセージに対するユーザーの操作情報も送信されます。また、ログ、ルールセット、G Data製品のバージョン番号も送信されます。

収集された情報の使用方法は?

有害度の数値（チェックサムによって識別）は、有害なファイルをG Dataが保するマルウェアデータベースでの照合に使用します。このファイルは、ピンポイントで分析され、場合によっては、ブラックリストでブロックされます。ユーザーの操作情報は、誤検出の発見や修正に役立ちます。

・G Data マルウェア情報イニシアチブの収集データのデータ保護に関する声明

上で述べた保護コンポーネントで必要なデータを除き、マルウェアイニシアチブでは、参加に協力頂いたユーザー様から、以下の情報を収集しています。これらの情報は、保護メカニズムの分析・開発の迅速化に役立つので、ぜひ参加にご協力ください。

G Data マルウェア情報イニシアチブとは?

G Data セキュリティラボでは、G Data 製品をご利用のユーザー様を、コンピュータの安全性を脅かす脅威からから保護するため、保護・対策の研究や分析に絶え間なく励んでいます。 マルウェア研究では、マルウェアに関する情報が多ければ多いほど、効果的な保護メカニズムの開発をいち早く進めることができます。これらの情報をG Data の研究・分析・開発に効率的に取り入れることを可能にするための取り組みが、G Dataマルウェア情報イニシアチブです。 これに

より、マルウェアに関するデータをG Dataセキュリティラボに送信することができます。 より多くのユーザー様に参加頂くことで、他のG Data製品をご利用の方々もインターネットをより安全に利用できるようになります。

収集される情報の種類は?

原則として、次の３種類のデータ収集方法があります。

1. G Dataの保護メカニズム（ウイルススキャナ、ふるまい検知、バンクガードなど）が、ユーザー様のコンピュータ上で有害ファイルが検出された場合（送信する情報は保護メカニズムによって異なります）

2. ウェブサイト上で有害なコンテンツが発見された場合

3. ユーザー様自身が任意でG Data セキュリティラボにデータを送信した場合

ユーザー様がマルウェアファイルをG Data セキュリティラボへ送信すると、システムは送信されるファイルのほかに、ワクチン情報、スキャンエンジンのバージョン番号、発見場所、オリジナルのファイル名、作成日という情報が一緒に送信されます。

有害なインターネットコンテンツを検出した場合は、次のデータが送信されます。

- マルウェア情報のバージョン
- G Data 製品および使用スキャンエンジンのバージョン番号
- 使用しているOSの言語
- コンピュータのIPアドレス匿名化のためのハッシュ
- ブラウザのユーザーエージェント
- アクセスを遮断したURLと遮断した理由（マルウェアサイト、フィッシングサイトなど）
- マルウェア名

不審な実行可能ファイルが検出された際は、次の情報を取得します。また、検出したファイルは、送信することもできます。

- 有害または不審なファイルのチェックサム
- ファイルサイズ
- ファイルに署名されている場合は、証明書の情報

- 攻撃に関わった有害または不審なファイルの検出場所
- 使用しているOSの言語
- コンピュータのIPアドレス匿名化のためのハッシュ
- 攻撃後に削除されたファイルの匿名パス
- 特定の条件下（G Dataが未所の新たな脅威が発生した場合）では、攻撃に関わったファイルのダウンロードをG Dataが要求することができます。送信されるファイルは、攻撃に関わっている実行可能なファイルのみです。

重要： 収集される情報には、個人情報は含まれません。また、取得した情報を使って個人の特定を行うことはありません。

収集したデータの利用方法は?

データの処理および保存にあたっては、各国で適用されるデータ保護ならび開示に関する法規が適用されます。 G Dataは、すべてのデータを不正アクセスから保護するため、厳重にデータを管理します。

ウェブサイトのアドレス情報は、まず選定が行われますが、有害または詐欺サイトの共通点を突き止める用途に使用されます。分析結果はURLブラックリストやG Data の他の保護メカニズムにも反映されます。特定のデータは、統計分析や開発などに使用されます。

不審なファイルに関する情報は、G Data で関連ファイルとの照合や有害プログラムの挙動を分析に使用します。取得した情報は、詳しい分析を行うためのベースとなる重要な要素です。目的は、保護メカニズムによる保護や駆除機能の改善となります。

有害プログラムの挙動を検証するには、有害ファイルが必要です。このため、ファイルをG Dataに送付することができます。送信するファイルは、実行可能なファイルのみです。文書やデータベースなど個人情報を含むファイルは送信されません。更に、ファイルは２つのステップを踏んで送信されます。まず、最初のステップでは、チェックサムもしくは他の共通プロパティを用い、ファイルをリクエストリストに入れられます。ファイルが再びリクエストされると、アップロードが開始されます。これが第２のステップです。このリクエストが同じコンピュータから発生するケースはほぼありません。ファイルは、その後G Data セキュリティラボで詳しく検証されます。統計データは、優先度の決定（例：頻度が高いほど、優先的に処理）、またはG Dataが作成するレポートに活用されます。マルウェアを削除するツールも、同様となります。

データの評価はG Dataセキュリティラボ内で行われ、評価結果はITセキュリティ分野の研究事案の解明にのみ利用されます。 収集データ利用における最大目標は、安全上のリスクの研究と保護メカニズムの開発です。 収集したデータの評価結果は例えば、ブラックリストの作成、専門記事発表のための統計、セキュリティ技術用ルールの開発などに利用されます。 このイニシアチブへの参加は任意であり、参加されなくてもご利用頂く製品の機能に影響がでることはありま

せん。 G Dataマルウェア情報イニシアチブにご参加頂くことにより、今後すべてのG Dataユーザーがコンピューターへの脅威について、より詳細な情報を得ることができるようになるとともに、ご利用のコンピュータの保護精度が向上します。

G Data製品によるデータ収集へのご理解とマルウェア情報イニシアチブ参加へのご協力頂きますよう、何卒宜しくお願い申し上げます。

使用許諾契約・コピーライト

G Data Software AG （以下、「G Data」）は、本使用許諾契約書のすべての条項に同意することを条件に、本ソフトウェア（以下、「本製品」）の使用許可をユーザー（以下、「ライセンス契約者」）に保証します。本使用許諾契約書に同意することによって、ライセンス契約者とG Dataの間に法的契約が締結されます。契約書の内容をよくお読みになってから、本製品をご利用ください。本契約書の条項に同意しない場合は、インストールを中断し本製品をお使いにならないでください。

1. 定義

「定義ファイル更新」： 製品の認証後にインターネット経由で利用できる機能（例： ウイルス定義ファイル（またはワクチンとも呼ぶ）、アンチスパム用のルール、URLリストなど）

「ドキュメンテーション」： 本製品に付属する関連文書

「ライセンス文書」： ライセンス数やライセンス効期限が記されているG Dataライセンス証明書、G Dataにより発行されたライセンス文書、あるいはライセンス契約者とG Dataとの間の書面による同意書。個人版製品では、ライセンスの適用範囲はパッケージなどに記されています。

「ソフトウェア更新」： インターネット経由で利用できるソフトウェアの新しいバージョンへの更新

「ライセンス」： ソフトウェアを利用できるPC（物理および仮想）の数量。デバイスのRAMにロードもしくはハードディスクなどの記憶領域にインストールされている状態を、ライセンスが「使用されている」とみなします。

「アクセスデータ」： 本製品に含まれているレジストレーション番号、レジストレーション番号の登録後にG Dataから送信されるユーザー名およびパスワード（定義ファイル更新もしくはソフトウェア更新の実行に必要）

2. 使用権

本使用許諾契約書では、G Dataはライセンス契約者に対して、ライセンス文書に記述されているライセンスの数量と効期間で許可される限りにおいて、非独占的、限定的、かつライセンス契約者の所属企業内部での委譲可能な使用権を許諾します。ライセンス契約者は、バックアップ目的での本製品の複製する権利をします。使用権の範囲は、G Dataのライセンス文書で定義された使用期間のすべてのソフトウェア更新および定義ファイル更新に及ぶものとします。

ライセンス契約者は、契約で合意したライセンス数を最大として、本製品をコンピュータにインストールし利用できるものとします。ライセンス文書はライセンス契約者が所持するライセンス数の証明となる文書です。

ライセンス契約者は、本使用許諾契約書の許諾事項を除き、G Dataによる書面の許可なく、（i）本製品の複製、改変、レンタル、リース、サブライセンスの譲渡、または利益の取得や未取得に関わらず、その他の手段を利用して第者に本製品を譲渡、（ii）本製品をベースに派生製品を開発、（iii）リバースエンジニアリング、逆アセンブルまたは逆コンパイル、（iv）第三者へアクセスデータを開示、する権限をさないものとします。

3. 所権

本製品の所権はG Dataもしくはライセンス提供者に帰属し、本製品は著作権法およびその他の知的財産権や国際条約によって保護されています。本製品の複製、修正、拡張および同製品の関連品に関するすべての権利は、G Dataおよびライセンス提供者に帰属し、ライセンス契約者は、これに同意するものとします。上記2の条項における本製品の使用権は、製品の購入によりライセンス契約者に移ります。

4. 保証

G Dataまたは販売代理店は、本製品を記録した記憶媒体もしくはダウンロードによる配布時において、ライセンス契約者に対し、通常の操作および保守条件下においてのみ、媒体もしくはダウンロードした製品がエラーなく動作することを保証します。万一、データ媒体もしくはダウンロードした製品にエラーが存在する場合は、G Dataもしくは販売代理店の定める保証期間内であれば、購入者は代替品の引渡しを要求できるものとします。上記の保証は、事故、不正利用、許可されていない修正、変更、拡張、または不適切な利用方法に起因する損害には適用されません。

上記に明示した保証は、適用される法律の許す限りにおいて唯一かつ排他的な保証であり、特定目的や商品性の保証を含め、その他のあらゆる明示的、黙示的保証に代わるものとします。G Dataは、本製品がライセンス契約者のあらゆる要求を満たす、あるいは如何なる環境においてもエラーが生じることなく動作することを保証しかねます。G DataおよびG Dataのライセンサー、ライセンシー、サプライヤー、または販売業者は、重大過失または明確に法律によって定義された状況を除き、本製品の使用または本ライセンス契約書に直接的または非直接的に関わらず、ライセンス契約者に生じた物質的・非物質的な損害に対し、一切の責任を負いません。なお、補償額は本製品の購入金額を限度とし、人的損害の場合は関連法規に準拠するものとします。

ライセンス契約者は、本製品の利用に関わるあらゆる法規および規定を遵守する責任を負い、本ライセンス契約書の受諾によってこれらを遵守することに同意するものとします。

5. テクニカルサポート

本製品のサポートは、G Dataもしくは販売代理店のサポートもしくはメンテナンスポリシーに準じて提供されるものとします。

6. ライセンス契約の解除

本使用許諾契約は、ライセンス契約者が本契約の条項を遵守しなかった場合、事前の通知なく自動的に失効するものとします。契約者は使用権が失効した時点で、ライセンス契約者は本製品の使用と本製品が記録された媒体を破棄するものとします。

7. 譲渡

事前にG Dataと書面同意し、ユーザーが使用許諾に同意した権利のすべてを譲渡する場合においてのみ、ライセンス契約者は、本契約で保証されている権利とライセンス契約を第者に譲渡できます。

8. ライセンス使用状況の検証

G Dataは、本製品が本使用許諾契約およびライセンス文書に準じた使用を確認するため、通常営業時間に基いた適切な事前通知および最大で1年に1回の履行頻度を条件に、G Dataが任命した守秘義務を課せられた監査人に、ユーザーの本製品に関するインストール状況とその記録の検証を依頼できるものとします。当該検証調査で発生する費用は、ライセンス契約者が使用許可されているライセンス数より5%超過したライセンスを使用している場合を除き、G Dataが負担するものとします。ライセンス契約者が許可されているライセンス数を超過して利用している場合は、ライセンス契約者は当該ライセンスの調査で発生した費用、および超過ライセンス分のライセンス料を負担するものとします。

9. 準拠法

本ライセンス契約書は、ドイツ連邦共和国の法律の解釈に従い、国際物品売買契約に関する国際連合条約の適用は除外されるものとします。本ライセンス契約で定められた一部もしくはすべての規定が無効、またはG Dataにより履行不能である場合でも、本ライセンス契約の残りの規定は引き続き拘束力をするものとします。本契約で定められた権利に対し違反が認められたにも関わらず、G Dataが権利履行を拒絶したとしても、以降の権利放棄を認めるものではありません。

10. サードパーティーのソフトウェア

本製品の一部には、オープンソースおよびフリーライセンスなどのサードパーティーにより開発されたソフトウェアが含まれています。本ライセンス契約は、上述のオープンソースおよびフリーライセンスに適用される権利または義務に対し効力を持ちません。相違する記述または異なる解釈がある場合、本ライセンス契約書の保証制限および保証排除はサードパーティーのソフトウェアに適用されます。

11. 個人情報の取り扱い

a) お客様に関する個人情報は、G Dataが必要な保護措置を講じたうえで、保、利用することにお客様は同意します。

- メールアドレス等、ユーザー登録時に届け出た事項及び、お客様から提出された問い合わせ内容およびアンケートへの回答内容等

b) G Dataが行うサービスにおいて、以下の目的のために個人情報を利用することにお客様は同意します。

- サポートサービスの提供、契約の更新案内、サービスに関する案内（セキュリティ情報等）、G Dataのパートナー他社製品の案内、各種調査、およびキャンペーン、イベントに関する案内、ベータ版テストの依頼等に関する案内

c) G Dataが前項を実施の際、秘密保持契約書を締結したうえで関連会社、販売代理店ならびに代行業者に対し個人情報を開示する場合があることにお客様は同意します。

12. その他の同意事項

本契約および本製品のライセンス文書は、ライセンス契約者とG Dataの間に締結される完全かつ排他的な同意書であり、あらゆる口頭書面による事前同意およびその他の合意における解釈に取って代わるものとします。本契約は、ライセンス契約書もしくは別途作成され、G Dataとライセンス契約者に署名されたライセンス文書もしくはその他の書面による取決めによってのみ、更できるものとします。

Copyright © 2013 G Data Software AG
Engine: The Virus Scan Engine and the Spyware Scan Engines are based on BitDefender technologies © 1997-2013 BitDefender SRL.
OutbreakShield: © 2013 Commtouch Software Ltd.
[G Data – 2013/06/24, 16:11]

索引

1
1 - 10 minutes 58
1st Boot Device 112

2
2nd Boot Device 112

A
About 14
About network 34
Access 42
Access data lost? 6
Access denied 119
Action if no rule applies 41
Activate later 6
Activate licence 75, 76
Adaptive mode 41
Add 47, 50, 94
Add to blacklist 16
Add to whitelist 16
Addresses/Domains 94
Advanced 68, 73, 78, 81, 84, 90
advanced editing mode 42
Advanced rule set editor (expert mode) 38
Advanced settings 98
After the installation 12
Allow 31
Allow this time 123
Also filter attachments in embedded email 99
Always allow 123
Always block 123
Analysis scope 88
AntiSpam 94
AntiVirus 65
Append report to received, infected mails 83
Application 106
Application radar 31
Application, if at least x inquiries are pending 106
Apply exceptions to idle scan 71
Approve time 53, 54
Automatic 104
Automatic start 58
Automatic virus checks 85
Automatically update virus signatures 75
Autopilot 16, 31, 104
Autopilot mode 104
Autostart Manager 22, 58
Autostart with delay 58
Autostart without delay 58
AUTOSTRT.EXE の実行 6
Avoid browser timeout 81

B
Backup 22
Backup restore 28
BankGuard browser protection 78
Behaviour monitoring 65
Betreff 99, 103
BIOS 112
Block periods 53, 54
Block this time 123
Block time 53, 54
Blocked networks 35, 36
Boot medium 28
boot scan 6, 28, 112
Boot scan using the program CD 113
Boot scan with G Data software that you have downloaded from the Internet 113
Booting from CD/DVD-ROM 112
Booting from USB stick 112
Both engines 65, 70, 90
Buy now 22, 127

C
Cancel 113
CD/DVD installation 6
CD/DVD からのブート 112
CD/DVD-ROM:, C: 112
CD版製品でのブートスキャン 113
Change 94, 97
Change security / performance 16
Changing computers 128
Check a program at startup 109
Check archives 68, 73, 90
Check computer 16, 113
Check computer (all local drives) 25
Check directories/files 25
Check email archives 68, 73, 90
Check emails before sending 83
Check for dialers / spyware / adware / riskware 68, 73, 90
Check for rootkits 25, 73, 90
Check for unprotected networks 106
Check for viruses 12
Check incoming email 83
Check memory and Startup 25
Check network access 68
Check removable media 25
Check system areas 73, 90
Check system areas during change of medium 68
Check system areas during system start 68
Close 113, 119
Comments 42
Complete 6
Content filter 99
Copyright 136
Create boot medium 28
Create G Data boot medium 113
Create new user 46
Create rule sets 34, 36
Create rules manually 104
Customize installation 6

D

Data safe 22
Days/hh:mm 52, 53
Define exceptions 16, 78, 80
Define rule 106
Delete 16, 27, 35, 55, 80, 94, 99, 111
Delete file 119
Delete infected file 122
Delete logs 56, 111
Description 50
Direct Internet connection 35, 36
Direction 38
Direction of connection 42
Disable automatic updates 16
Disable autopilot 16, 117
Disable behavior monitoring 16
Disable email protection 16
Disable firewall 16, 117
Disable HTML scripts 99
Disable idle scan 16
Disable monitor 117
Disable spam protection 16
Disable virus monitor 16
Disable web protection 16
Disinfect 27
Disinfect (if not possible: delete attachment/text) 83
Disinfect (if not possible: delete file) 119
Disinfect (if not possible: log only) 119
Disinfect (if not possible: move to quarantine) 122
Disinfect (if not possible: place in quarantine) 65, 70, 90, 119
Display help 14
Display warning before time expires 53
Do not launch 58
Do not run on batteries 89
Do not switch off computer during manual virus check 73
Download size limit 81

E

Edit 33, 35, 36, 42, 45, 55, 99
Edit blacklist 16
Edit network 34
Edit rule 42
Edit rule set 34
Edit whitelist 16
Email check 16, 82
Email text 99, 103
Embedded emails 99
Enable automatic configuration (DHCP) 34
Engine 62
Enhance range of functions 22
Enter a new registration number 6
Enter access data 6
Exceptions 47, 67, 71
Exceptions for on-demand scan 71
Execute actions 119
Exit 125
Export 16, 94
Extend licenses 22
Extras > Scan folder for viruses 84

F

FAQ: boot scan 112
FAQ: License questions 127
FAQ: Program functions 117
Fast check 12
File and printer sharing 38
File extensions 99
File types 73, 90
Files with the extension PST 122
Filter malicious attachments 99
Filters 47, 50
Firewall 16, 22, 30, 104
Firewall | Networks 31
Firewall alarm 36, 42, 123
Firewall disabled 104
Firewall enabled on this network 34
Firewall logs 111
First steps 4
Folder name 97, 99
Full version 6

G

G Data AntiVirus - Alternative 113
G Data AntiVirus(もしくはG Data BootMedium) 113
G Data Backup (restore) 28
G Data アイコン 117
G Data バックアップ（復元） 28
G Data ブートスキャン 113
G Data（製品名）を起動 117
G Data boot CD 113
G Data boot CD – alternative 113
General 62, 87
Generate a rule set which contains a number of basic rules 36
Generate an empty rule set 36
Generate log 73, 75, 90
Global functions 14

H

Header 99
Heuristics 68, 73, 90
High security 104
High spam probability 97
How do I cancel a boot scan? 112

I

IMAPI 2.x がインストールされていません 113
Import 16, 94
In entire text 47
In the case of an infection 83
Incoming mail 83
Infected archives 65, 90
Infected files 65, 70, 90

Insert message in email text 99
Insert spam warning in mail subject and mail text 97
Insert warning in mail subject and text 99
Installation 6, 45
Internet connection sharing 34, 38
Internet settings 75, 76, 77, 94
IP range 42
IP アドレス範囲 42

J

Job 87

L

Language filter 99
Last idle scan 16
Last update 16
Licence 22
Licence renewal 127
Link to site 50
Load settings 61
Log 42, 56, 119
Log only 119, 122
Log: No spam 16
Log: Spam 16
Logged in successfully 76
Login 76
Logs 14, 75, 111, 119
Low security 104

M

Malware Information Initiative 6, 27
Manual virus check 70
Match to applications 42
Match to Internet service 42
Maximum security 104
Meta 47
Microsoft Outlook 16, 97
Microsoft Windows 112
Minimal 6
Miscellaneous 103, 109
Mode 31, 68
Monitor computer usage period 45, 53
Monitor exceptions 67
Monitor Internet usage period 45, 52
Monitor status 65
More filters 99
More settings 16, 31
Move back 27
Move file to quarantine 119, 122
Move mail to folder 97, 99
Multi-user licenses 127

N

Name 41, 42
NetBIOS 38
Networks 30, 31, 33
New 16, 35, 36, 42, 47, 50, 55, 67, 71, 80, 85, 99
New user 45, 46
Next update 16
Not a virus message 125
not-a-virus 125
Note 64, 80

O

Offer to use autopilot mode when launching a full screen application (game mode) 104
Offer virus checking for removable data media 73
OK 47, 50, 80, 127
On system start-up 89
Only check new or modified files 68, 73
Only rename attachments 99

Other

Other POP3 email clients 103
OutbreakShield 83
Outgoing mails 83
Parental controls 22, 45
Parental controls for this user 45
Parental controls logs 111
Password 64
Password hint 64
Password-protected archives 119
Pause the virus check at times of high system load 70, 119
Perform reference checking for loaded modules 108
Permitted content 45, 50, 55
Personal filters 47, 55
Phishing protection 78
Plus 25
Port 38
Prerequisites 112
Prevented attacks 31
Print 111
Program path 38
Prohibited content 45, 47, 55
Properties 60
Protect more PCs / Enhance range of functions 22
Protocol/Port/Application 106
Proxy server 77
Quarantine 65, 119
Quarantine and mailboxes 122
Quarantined files 27, 119, 122
Queries 106
Query table contents 94
Rank 42
Reaction 97, 99
Real-time protection 16, 65
Re-enter password 64
Reference testing 108
Reject mail 97, 99
Remove password 64
Repeat application queries 106
Reset settings 61
Reset tables 94
Return 112

Rule enabled 42
Rule set 34
Rule set name 36
Rule sets 30, 33, 35
Rule wizard 42
Rules 42
Run 89
Run AUTOSTRT.EXE 6
Run job automatically on next system startup if system was powered off at the scheduled start time 89
Run virus check 119
Save 111
Save connection log 109
Save settings 61
Scan folder for viruses 16, 82
Scan options 83
Scan settings 90
Scan unread mails at program start 103
Scan web content (HTTP) 78
Scheduled virus checks 85
Scheduling 89
Search criterion 99
Search location 47
Search scope 99
Security 31
Security icon 12, 117
Security status 14
Security/performance 62
SecurityCenter 14, 22, 75, 117, 127
Select directories/files 88
Selection 88
Sender addresses/sender domains 16
Sender filter 99
Sender/domains 99
Server port number 84
ServiceCenter 4, 5, 6, 14
Set delay 58
Settings 14, 61
Settings | AntiSpam | Spam filter 16
Settings | AntiVirus | Email check 16
Settings | AntiVirus | Real-time protection 16
Settings | AntiVirus | Updates 16
Settings | AntiVirus | Web protection 16
Settings | Firewall | Automatic 16, 31
Settings | Other 36
Settings: 14, 30
Settings: Log 111
Settings: Manual virus check 119
Settings: Miscellaneous 111
Setup 6
Setup.exe 6
Share or block applications 38
Share or block domain services 38
Share or block network services 38
Share or block VPN services 38
Show quarantine 27
Shredder 12
Slow computer 62
Software download 6
Software modules 22
Spam filter 94
Spam OutbreakShield 94
Spam protection 16
Standard 84
Standard computer (recommended) 62
Standard security 104
Start G Data software 117
Start idle scan now 16
Start time 111
Statistics 117
Status 30, 31, 111
Status displays 16
Stealth mode 41
Step 1 - Starting the installation 6
Step 2 - Selecting the language 6
Step 3 - Installation methods 6
Step 4 - License agreement 6
Step 5 - User-defined installation (optional) 6
Step 6 - Software version 6
Step 7 - Product activation 6
Step 8 - Finishing the installation 6
Step-by-step execution 113
Submit 27
Submit URLs of infected websites 78
Suffix 99
Suspected spam 97
Switch off computer after virus check 119
Switch off the computer after completion of the job 87
The email [subject line] contains the following virus: [virus name] 83
The message has been rejected 103
Time 89
Time window 42
Title 47, 111
Tools 82
Trusted networks 35, 36
Tuner 22
Type 111
Typical 6
Unable to activate your license? 76
Uninstall 125
Unknown server applications 106
Untrusted networks 35, 36
Update 16, 27
Update complete 113
Update software 14
Update virus signatures 16, 117, 127
Updates 6, 14, 75
URL 47, 80
USBメモリを利用したブートスキャン 113
Use blacklist 94
Use content filter 94
Use engines 65, 70, 83, 90
Use keywords (mail text) 94
Use keywords (subject) 94

Use proxy server 77
Use real-time blacklists (default setting) 94
Use spam filter 94
Use the rule wizard 38
Use whitelist 94
User 45, 46
User account 93
User-defined 6, 62
User-defined security settings 104
User-defined update 6
Using the advanced editing mode 38, 41
Very high spam probability 97
VIRUS 83
Virus alarm 122
Virus check 16, 25, 117
Virus protection 14, 22, 25, 119
Virus protection logs 111
VPN 38
VPNサービスを許可/拒否 38
Warning! This mail contains the following virus 83
Web protection 16, 78
What happens on license expiration? 22
Windows ユーザーアカウント 46
Wizard default settings 109
www.gdatasoftware.com 5
Yes 113
Your computer starts differently than usual after installing the software 12
アイドリングスキャンを使用 16
アイドリングスキャンを無効にする 16
アクセス 42
アクセスデータ 6, 127
アクセスデータの確認 6
アクセスデータを入力 6
アクセスを拒否するネットワーク 35, 36
アクセス拒否されたファイル 119
アダプティブモード 41
アプリケーションレーダー 31
アプリケーションを許可/拒否 38
アプリケーション割当て 42
アラート 42
アラートにより作成 42
アンインストール 125
アンインストールの方法 125
アンチウイルス 22
アンチウイルスのログ 111
アンチスパム 16
アンチスパムを無効にする 16
インストール 6
インストールの完了 6
インストールの開始 6
インストール方法の選択 6
インターネットサービス割当て 42
インターネットに直接接続 35, 36
インターネット利用時間の監視 52
インターネット接続共有 34
インターネット接続共有を許可/拒否 38
ウイルスガード 16
ウイルスガードを無効にする 16, 117
ウイルスが検出されたら 113
ウイルスが検出された場合 119
ウイルススキャン 25
ウイルススキャンで「not-a-virus」が表示される 125
ウイルススキャンの流れ 119
ウイルス検出時の対応 122
ウイルス駆除 27
ウイルス駆除（不可能な場合はアクセスをブロック） 122
ウイルス駆除（不可能な場合はファイルを削除） 119
ウイルス駆除（不可能な場合はログを残すのみ） 119
ウイルス駆除（不可能な場合は隔離） 119, 122
ウェブ保護 16
ウェブ保護を無効にする 16
オートスタートマネージャー 22
オートパイロット 16, 31
オートパイロットを無効にする 16, 117
カスタムインストール 6
このネットワークでファイアウォールを有効にする 34
このユーザーのフィルタリング 45
コメント 42
コントロールパネル 125
コンピュータをスキャン 16, 25

コンピュータを買い替えたり、クリーンインストールした場合 128
コンピュータ利用時間の監視 53
サイトへのリンク 50
システム負荷が高い時はウイルススキャンを停止 119
スキャン終了後にコンピュータの電源を切る 119
ステータス 16, 30, 31, 111
ステルスモード 41
セキュリティ 31
セキュリティ / パフォーマンス 16
セキュリティステータス 14
セキュリティセンター 22
セキュリティを編集 31
タイトル 47
ダウンロード版製品でのブートスキャン 113
チューナー 22
データセーフ 22
データセーフを開く 117
データ保護に関する声明 129
デフォルトルール 42
ドメインサービスを許可/拒否 38
ネットワーク 30, 31, 33
ネットワークサービスを許可/拒否 38
ネットワークについて 34
パーソナルフィルタ 47, 55
パーソナルフィルタを作成 47, 50
パス 38
パスワード保護されたアーカイブ 119
バックアップ 22
ファイアウォール 16, 22, 30
ファイアウォールのログ 111
ファイアウォールを無効にする 16, 117
ファイルアクセスをブロック 122
ファイルおよびプリンタ共有を許可/拒否 38

ファイルが__KBに達したときにメッセージを表示　56
ファイルを隔離　119, 122
フィルタ　47
フィルタリング　22, 45
フィルタリングのログ　111
ブート　112
ブートスキャン　28, 112
ブートスキャンの流れ　6, 113
ブートスキャンの準備　112
ブートメディア　28, 112
ブートメディアを作成　28, 113
フォルダ/ファイルをスキャン　25
ブラックリスト　55
ブラックリストを編集　16
ふるまい検知を無効にする　16
プログラムと機能　125
プログラムの追加と削除　125
プロトコル　42
ヘルプを表示　14
ポート　38
ホワイトリスト　50, 55
ホワイトリストを編集　16
マルウェア情報イニシアチブ　6, 129
マルウェ情報イニシアチブ　27
メールボックスの隔離に関しての注意　122
メール保護　16
メール保護を無効にする　16
メタタグ　47
メモリとスタートアップをスキャン　25
ユーザー　46
ユーザーサポートについて　5
ユーザーの接続履歴　111
ユーザー名とパスワード　127
ライセンス　22
ライセンスの有効期間が切れた場合　22
ライセンスの期限が切れた場合　127
ライセンスの移行　128
ライセンスの認証　6
ランク　42
ランク順　42
リアルタイム保護　16
リムーバブルメディアをスキャン　25
ルートキットをスキャン　25
ルール　36, 42
ルールウィザード　38, 42
ルールセット　30, 33, 34, 35, 36, 41
ルールセットを編集　34
ルールセット名　36
ルールにないアクセスが検知された場合の操作　41
ルールを編集　42
レジストレーション番号　6
レジストレーション番号を入力　6
ログ　14, 111
ログ: スパム　16
ログ: スパム以外　16
ログを削除　56, 111
ログを残すのみ　119
ワクチンの更新　16
ワクチンを更新　117
今すぐ実行　16
体験版として登録　6
使用許諾契約　6
使用許諾契約・コピーライト　136
例外　47
例外を設定　16
保護する台数を増やす　22
信頼性の低いネットワーク　35, 36
信頼性の高いネットワーク　35, 36
元に戻す　27
共通機能　14
内容　111
削除　27, 111, 119
前回のウイルススキャン　16
前回のワクチン更新　16
動作環境　6
印刷　111
名前　41, 42
名前を付けて保存　111
変更　6
完全アンインストールツール　6
後で認証を行う　6
復元　28
情報　14
感染ファイルを削除　122
手動でルールを作成　31
拒否されたコンテンツ　111
拡張ルールセットエディタ　38, 41, 42
拡張ルールセットエディタへ切換え（エキスパートモード）　38
接続の方向　38, 42
推奨ルールを含むルールセットを生成　36
撃退した攻撃　31
操作　119
操作の実行　119
操作を実行　119
新規ユーザー　46
新規作成　36
時間　42
時間切れの前に警告を表示　53
更新　27
有効なルール　42
検索対象　47
次回のワクチン更新　16
理由　111
禁止するコンテンツ　45, 47, 55
禁止する基準　47
禁止する時間　53, 54
種類　111
空のルールセットを生成　36
統計情報　117
編集　33
自動（オートパイロット）　31
自動再生　6
自動更新を無効にする　16
自動設定を有効にする（DHCP）　34

製品版として登録　6
製品種類の選択　6
複数台用ライセンス　127
複数台用ライセンスを所有している場合　127
設定　14, 30
設定 | ファイアウォール | 自動　31
設定:ログ　56
許可するコンテンツ　45, 50, 55
許可する時間　53
詳細　111
詳細設定　16, 31
説明　50
送信　27
開始時刻　111
隔離　27, 119
隔離されたファイル　27
隔離領域　119, 122
隔離領域を表示　27
駆除できない場合　119